

La Société de Surveillance ; mythe ou réalité au sein des pratiques judiciaires de traçabilité numérique?

Mémoire réalisé par
Hadrien BROOMS

Promoteur
Marie-Sophie Devresse

Année académique 2015-2016

Master en criminologie à finalité spécialisée : criminologie de l'intervention

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **<http://www.uclouvain.be/plagiat>**.

Remerciements

Un tout grand merci

à Marie-Sophie Devresse, promotrice de ce mémoire, pour le temps consacré à mes demandes, ses conseils aussi avisés que judicieux et ses nombreuses lectures ;

à Nicolas Rongveaux qui m'a apporté son support moral et intellectuel tout au long de ma démarche ;

à l'ensemble des protagonistes interrogés lors de mes recherches sans qui celles-ci n'auraient abouti ;

aux proches qui ont eu la gentillesse de relire ce travail

et à toutes les personnes ayant permis l'aboutissement de mon mémoire.

Table des matières

INTRODUCTION GENERALE.....	1
PREMIERE PARTIE : Méthodologie.....	4
1. Introduction.....	5
2. Le projet de recherche.....	6
2.1. Le contexte.....	6
2.2. La question de départ et les objectifs de recherche.....	6
3. La délimitation du champ de recherche.....	7
3.1. Les acteurs interrogés.....	7
3.2. Le cadre spatio-temporel.....	8
4. Les méthodes de recueil des données.....	9
4.1. L'analyse documentaire.....	9
4.2. L'entretien de recherche semi-directif.....	10
4.2.1. La structure des entretiens.....	11
4.2.2. Les difficultés rencontrées.....	11
5. L'analyse de l'information	13
5.1. Le modèle d'analyse.....	13
5.2. La méthode d'analyse de l'information.....	14
DEUXIEME PARTIE : Émergence de la Société de Surveillance.....	16
1. Introduction.....	17
2. Les facteurs d'émergence de la Société de Surveillance.....	19
2.1. Le risque, objet d'une attention grandissante dans la société contemporaine.....	19
2.2. L'obsession sécuritaire à la suite d'événements catalyseurs.....	21
2.3. La militarisation de la surveillance.....	24
2.4. L'économie politique de la surveillance.....	26
2.5. L'économie de l'information personnelle.....	28
3. Conclusion.....	30
TROISIEME PARTIE : Étude de la Société de Surveillance.....	31
1. Introduction.....	32
2. Un premier regard sur la Société de Surveillance.....	34

2.1. Définitions.....	34
2.2. « What is wrong with a Surveillance Society ? ».....	36
2.2.1. Deux confusions à éluder.....	36
2.2.2. L'ambivalence des effets de la surveillance.....	39
3. Les mécanismes de la Société de Surveillance.....	41
3.1. Le partage de l'information.....	41
3.1.1. La base de données.....	43
3.1.1.1. La base de données dans la loi belge.....	44
3.1.1.2. Le fonctionnement d'une base de données.....	47
3.1.1.3. Un cas illustratif : le Passenger Name Record.....	48
3.1.2. La contribution des entreprises commerciales.....	50
3.1.2.1. Le transfert volontaire de données.....	51
3.1.2.2. L'achat d'informations.....	52
3.1.2.3. L'usage de mécanismes juridiques.....	53
3.2. Le détournement d'usage.....	56
3.3. Le tri social, la catégorisation et le ciblage.....	58
3.3.1. Première illustration : les pratiques commerciales.....	60
3.3.2. Seconde illustration : l'e-cops.....	62
3.3.3. Illustrations non-exhaustives de tri social.....	63
4. Les nouvelles technologies de surveillance.....	65
4.1. Les technologies numériques de traçabilité.....	66
4.1.1. La téléphonie mobile.....	68
4.1.1.1. Téléphone portable et réseau cellulaire.....	69
4.1.1.2. La géolocalisation d'un téléphone portable.....	72
4.1.1.3. La fréquence et le coût de la géolocalisation téléphonique.....	75
4.1.2. La carte bancaire.....	78
4.1.2.1. La recherche bancaire.....	80
4.1.2.2. Le champ d'application de la recherche bancaire.....	81
4.1.3. La base de données commerciales.....	82
4.2. L'usage des technologies numériques de traçabilité dans l'enquête pénale.....	85
4.2.1. Les critères d'application.....	86
4.2.1.1. L'opportunité et la valeur ajoutée.....	86
4.2.1.2. Le coût de la mesure.....	87
4.2.1.3. La faisabilité technique.....	87

4.2.1.4. Le respect des normes juridiques en matière de vie privée.....	88
4.2.2. Le champ d'application.....	89
4.3. La synergie des technologies numériques de traçabilité.....	91
5. Conclusion.....	94
QUATRIEME PARTIE : Sommes-nous dans une Société de Surveillance ?.....	95
1. Introduction.....	96
2. Les obstacles à l'établissement d'une Société de Surveillance.....	97
2.1. Le manque de personnel et la quantité trop importante de données.....	97
2.2. Le manque de moyens financiers.....	99
2.3. De nombreuses contraintes juridiques.....	101
2.4. L'adaptation des délinquants aux mesures judiciaires de traçabilité.....	103
3. Conclusion.....	105
CONCLUSION GENERALE.....	106
BIBLIOGRAPHIE.....	109

Introduction générale

« *Ma faute est d'avoir eu des yeux* »
- Ovide ; *Tristes*, III, 5, v50.

À l'instar du petit poucet qui, dans le conte éponyme, semait des cailloux pour retrouver son chemin, l'*homo numericus* de notre époque laisse d'innombrables traces lorsqu'il se meut dans une société traversée de réseaux et qui réside pour une bonne part dans un royaume incorporel constitué d'informations pures. Un téléphone portable peut, entre autre, fournir à l'autorité compétente la localisation précise de son utilisateur grâce au truchement des bornes téléphoniques qu'il sollicite dans son activité. L'utilisation de cartes de crédit permet également de déterminer la présence d'un individu dans tel ou tel lieu à un moment précis. Présence qui pourra, le cas échéant, être confirmée par les caméras de vidéosurveillance positionnées aux quatre coins de l'espace public. Cette convergence de moyens de plus en plus sophistiqués pare de la sorte la personne du citoyen d'une forme d'ombre informatique, plus visible que lui-même pour qui la regarde, et qui pourtant le suit partout.

Les informations ainsi recueillies, de même que l'utilisation qui peut en être faite, sont loin d'être innocentes : plus que la localisation, ce sont désormais les comportements, les habitudes de consommation, les intérêts divers de l'individu qui sont examinés à la loupe.

De telles traces constituent assurément des données personnelles et pertinentes pour celui ou celle qui souhaite collecter toute une série d'informations sur l'Homme, sur ses comportements ou ses mouvements. Il est désormais possible pour celui qui en a les moyens de déterminer notamment les allées et venues, les trajets effectués et la localisation actuelle d'un individu ciblé. Parallèlement à la multiplication de ces traces, grâce au développement des nouvelles technologies, nous observons la mise en place d'instruments de récolte de ces données sous formes d'agrégats par différentes autorités, étatiques ou non, dont le leitmotiv est principalement la recherche d'une sécurité optimale, quitte à piétiner au passage le principe fondamental du droit à la vie privée. Ainsi, c'est par ce motif qu'on a justifié l'organisation de dispositifs de surveillance de l'Homme et des empreintes qu'il laisse dans son sillage. Le rôle des autorités judiciaires et des services de police dans ce processus ne peut être négligé : l'exercice de la force publique inclut aujourd'hui, dans une zone amniotique située aux frontières de la légalité – la réglementation de ces pratiques se faisant attendre –, l'utilisation du *big data* à des fins de surveillance et de reconnaissance.

« A notre insu, nous sommes de plus en plus observés, épiés, surveillés, contrôlés, fichés. Chaque jour, des technologies nouvelles affinent le pistage de nos traces »¹. L'essor du numérique inscrit la société dans une période singulière : celle de la transparence totale. Avec les développements technologiques, il devient dorénavant indispensable pour l'État et ses organismes de saisir et d'interpréter une telle transparence.

Devons-nous dès lors craindre une surveillance omniprésente ? Nous dirigeons-nous vers la société de surveillance totale de Georges Orwell décrite dans son célèbre roman *1984* ? Au vu des enjeux de sécurité qui ne cessent de se rappeler à nous ces dernières années, la surveillance n'est-elle pas, aujourd'hui, une nécessité ? Dans ce cas, à quelles conditions pouvons-nous faire confiance aux structures étatiques d'en user à bon escient ? Quels sont les tenants et aboutissants d'une surveillance indiscriminée menée par les acteurs judiciaires en Belgique ? Telles sont les interrogations qui s'imposèrent à notre égard et dont l'absence de réponse nous incita à conduire notre étude.

Axée sur l'éventuel établissement d'une société de surveillance à travers l'usage judiciaire des instruments de traçabilité numérique, notre recherche se scinde en quatre grandes parties.

La première partie de notre étude nous permettra de circonscrire et d'explicitier les objectifs initiaux de la recherche ainsi que la démarche dans laquelle elle s'est inscrite. Plus précisément, cette partie préliminaire présentera une description minutieuse de la méthodologie qualitative employée pour concevoir une telle étude. Nous nous appuierons dès lors majoritairement sur la délimitation du champ de recherche – les méthodes de recueil des données – et l'analyse des informations afin d'indiquer le cadre restreint de ce travail.

La deuxième partie de notre mémoire sera consacrée aux facteurs généraux ayant permis l'émergence d'une société de surveillance dans les pays occidentaux. Comme l'atteste David Lyon, une attention soutenue apportée à ces influences, leur poussée et leur inscription dans les structures modernes de la société permet de prendre utilement conscience de ce que les grands événements affectent bien le monde social². Nous estimons donc opportun d'aborder les mécanismes sous-jacents d'un phénomène pour en comprendre ses principales

¹ I. RAMONET, *L'empire de la surveillance*, Paris, Galilée, 2015, p. 13.

² D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », In *Au nom du 11 septembre... : les démocraties à l'épreuve de l'antiterrorisme*, sous la dir. de Didier Bigo, Laurent Bonelli et Thomas Deltombe, Paris, La Découverte, 2008, p. 93.

manifestations actuelles. Cette deuxième partie présentera par conséquent l'avantage d'amener le lecteur de ces lignes vers la partie subséquente de cette recherche armé des clés de compréhension nécessaires.

L'analyse de la Société de Surveillance constituera la troisième partie de cette étude. Considérée par une majorité de chercheurs comme un phénomène aux larges ramifications, nous analyserons ses principaux traits à travers la littérature pour en apprécier ses formes et contours. A cet égard, les chapitres de cette partie – les fondements d'une telle société en considération de sa définition et des confusions basiques à éluder, les différents mécanismes mobilisés au sein de celle-ci ainsi délimitée et les technologies numériques de traçabilité sur lesquelles reposent en partie ces mécanismes – offriront une description pertinente de la Société de Surveillance. L'objectif de cette partie principale sera donc d'illustrer par ses caractéristiques universelles ce qu'est une telle société de surveillance ; ces considérations étant nécessaires afin de pouvoir apprécier cette société à l'échelon local et permettant dès lors d'amorcer la dernière partie de notre étude.

La dernière partie sera consacrée à l'existence, ou non, de la Société de Surveillance sur le terrain de nos investigations. Nous mobiliserons à cette fin des ressources tant littéraires qu'issues de nos entretiens pour rencontrer, au terme de nos investigations, notre interrogation principale : pouvons-nous conclure à l'établissement, au sein du champ de recherche de ce mémoire, d'une telle société dans le cadre des pratiques de traçabilité numérique au sein d'une enquête pénale ?

Première partie :
Méthodologie

1. Introduction

*« On ne peut se passer d'une méthode
pour se mettre en quête de la vérité des choses »
- René Descartes ; *Discours de la méthode* (1637)*

Le mémoire est un exercice périlleux et de longue haleine, au cours duquel l'imprévision est la principale source d'égarement ; et, de même que l'architecte s'intéresse en premier lieu aux fondations, l'étudiant consciencieux commence par poser de solides bases à sa réflexion. L'édifice n'en est, dans un cas comme dans l'autre, que plus robuste. L'impérieuse nécessité est donc de se référer à des repères clairs et stricts – prenant la forme d'un fil conducteur méthodologique – en vue de présenter des résultats concrets et cohérents. Ainsi, lorsque l'on s'engage dans une recherche en sciences sociales, « il importe avant tout que le chercheur soit capable de concevoir et de mettre en œuvre un dispositif d'élucidation du réel, c'est-à-dire, dans son sens le plus large, une méthode de travail »³.

Avant d'aborder le cœur de notre étude, il est nécessaire d'en expliciter l'ossature par une présentation succincte de notre méthode de travail, inspirée, dans les grandes lignes, des écrits de Luc Van Campenhoudt et de Raymond Quivy. Pour ce faire, cette partie méthodologique se scinde en quatre chapitres distincts.

Tout d'abord, nous présenterons brièvement le projet de recherche dans le cadre duquel est née cette étude ; à savoir le contexte, la question de départ et les objectifs établis lors de ces essentielles prémices. Nous relaterons ensuite la délimitation du « champ de recherche » afin de situer notre contribution littéraire dans le vaste domaine des études consacrées à la société de surveillance. Ainsi, nous évoquerons, d'une part, les multiples acteurs interrogés et, d'autre part, le cadre spatio-temporel propre à nos investigations. Conséquemment à ces considérations, nous aborderons, dans un avant-dernier chapitre, les méthodes de recueil des données – comme l'analyse documentaire et les entretiens semi-directifs – mobilisées au sein d'un tel champ d'analyse. Enfin, nous clôturerons cette partie méthodologique par un commentaire sur le modèle d'analyse des données largement emprunté dans le cadre de ce mémoire.

³ L. VAN CAMPENHOUDT & R. QUIVY, *Manuel de recherche en sciences sociales*, 4^e éd., Paris, DUNOD, 2013, p. 7.

2. Le projet de recherche

Un projet de recherche constitue une assise solide sur laquelle peut reposer un mémoire. Son exposition permet d'en présenter la genèse et l'organisation originelle, nécessaire en vue d'explicitier l'orientation *ab initio* de l'étude voulue par le chercheur. Ainsi, nous commentons brièvement dans la suite de ces lignes le contexte et les objectifs initiaux de cette étude à travers sa question de départ.

2.1. Le contexte

La question de la surveillance, inhérente à la société contemporaine, s'est rapidement imposée à notre égard comme un sujet d'étude potentiel. Par la lecture exploratoire de certains ouvrages sur ce thème, nous avons en effet développé un réel intérêt tant pour la question de l'existence d'une société de surveillance généralisée que pour le fonctionnement et l'apport des nouvelles technologies de traçabilité numérique dans une enquête pénale. Mû par cet intérêt, nous avons souhaité approfondir nos connaissances. Toutefois, une interrogation majeure guidant les prémisses de nos recherches demeurerait en suspens : pouvions-nous confirmer l'établissement d'une telle société en Belgique eu égard au traçage des individus par les différents acteurs judiciaires ?

2.2. La question de départ et les objectifs de recherche

Notre question de départ s'énonce dès lors dans ces termes : « Quel est l'usage, opéré par la police fédérale belge, des modes de traçabilité par les objets numériques et techniques dans la recherche de personnes soupçonnées d'avoir commis une infraction ? ». À travers ce questionnement se dessinent plusieurs objectifs.

Plus précisément, l'un des objectifs de cette recherche vise à déterminer le recours systématique, ou non, par la police, aux méthodes de traçabilité des comportements humains. En d'autres termes, il s'agira d'apprécier qualitativement l'usage de ces moyens dans une enquête pénale. D'une manière plus générale, cette recherche tend également à préciser si, sous le prisme de la traçabilité, nous pourrions confirmer l'hypothèse d'une surveillance généralisée à un échelon local.

3. La délimitation du champ de recherche

La surveillance est un domaine extrêmement large. Si nous avons pu restreindre ce domaine par la constitution d'une question de départ et l'explicitation des objectifs initiaux, encore faut-il, pour des raisons d'ordre économique, inscrire notre étude dans un cadre limité de recherche. Autrement dit, il est primordial de délimiter minutieusement un tel champ en vue de mettre en place une analyse praticable et réaliste. Tel est le fondement de ce chapitre que nous avons souhaité développer dans les sections subséquentes afin de garantir le bon suivi de l'analyse. Dans un premier temps, nous aborderons les acteurs interrogés – principaux et secondaires – pour décrire, dans un second temps, le cadre spatio-temporel au sein duquel l'objet étudié s'intègre.

3.1. Les acteurs interrogés

Tout d'abord, nous avons déterminé le champ de recherche de notre étude sur base des acteurs que nous avons souhaité interroger dans le cadre de notre travail. Figurent en premier lieu, au sein de ce champ restreint, les juges d'instructions et les fonctionnaires de police. Ces acteurs professionnels sont particulièrement intéressants dans l'analyse des mesures de surveillance par les instruments de traçabilité des comportements humains. En effet, les premiers assument l'ordonnance de ces moyens d'enquête tandis que les seconds l'exécutent. En second lieu, se trouvent intégrés, au cœur de nos recherches, les agents de la cellule « coordination de justice » de chaque opérateur principal – Base, Mobistar et Proximus – de téléphonie mobile en Belgique. Chargés d'exécuter les réquisitoires de la justice adressés à ces entreprises, leurs témoignages offrent des renseignements éclairants en matière de repérage et de localisation d'un individu. L'ensemble de ces personnes constitue les *principaux* acteurs que nous avons interrogés.

S'insèrent également, dans notre champ de recherche, plusieurs acteurs *secondaires*. Nous avons ainsi questionné un expert judiciaire car une telle fonction implique de devoir travailler en étroite collaboration avec les juges d'instruction. Cette proximité avec les autorités judiciaires présente assurément l'avantage d'offrir un point de vue diversifié sur la mise en œuvre des mesures de traçabilité. En outre, le concours d'un agent de l'Institut belge des services postaux et des télécommunications a été sollicité dans nos recherches. Considéré

comme le régulateur des opérateurs de téléphonie mobile, cet institut peut intervenir dans certaines missions de géolocalisation d'un individu, au même titre que les agents de la cellule coordination justice. Finalement, nous avons interrogé deux chercheurs universitaires compétents dans les questions de surveillance. Notons que de tels acteurs s'inscrivent en marge de notre analyse et présentent une importance moindre en comparaison des précédents protagonistes. L'objectif poursuivi de s'entretenir avec ces professionnels consiste, dans les grandes lignes, à éclaircir certains points obscurs de la société de surveillance et à expliciter différents mécanismes complexes que représentent les mesures de traçabilité numérique.

3.2. Le cadre spatio-temporel

Après avoir déterminé les contours de notre recherche sous le prisme des acteurs interrogés, il nous semble opportun de préciser ensuite son cadre spatio-temporel. Pour des raisons de commodité personnelle, nous souhaitons nous en tenir aux limites territoriales des principaux arrondissements judiciaires – Hainaut (Tournai & Charleroi), Namur, Liège et Eupen – en Wallonie afin d'apprécier si la société de surveillance par le biais de la traçabilité y est opérante.

Certes, nous faisons couramment allusion, dans les parties suivantes, aux pratiques existant en dehors de ces limites territoriales, principalement en Europe et aux États-Unis. Ce détour nous est toutefois imposé par l'internationalisation de la société de surveillance ; un tel phénomène ne se limite en effet en aucun cas à des frontières territoriales prédéfinies. Pour en comprendre les ressorts, les mécanismes et en déterminer la possible existence à travers certaines pratiques judiciaires mises en œuvre au sein d'une zone territoriale prédéfinie – celle de notre cadre susmentionné – nous devons, en définitive, emprunter nécessairement un tel détour.

4. Les méthodes de recueil des données

Une fois le sujet circonscrit, il est nécessaire de procéder à la récolte de données pertinentes afin de produire un travail d'étude. À cette fin, plusieurs méthodes permettent au chercheur de se constituer un corpus riche et diversifié. Lors de nos investigations – axées sur la société de surveillance et les pratiques judiciaires de traçabilité – nous avons combiné deux méthodes de recueil de données : l'analyse documentaire et l'entretien de recherche semi-directif. Nous donnons dans les développements ultérieurs un bref aperçu de ces dispositifs.

4.1. L'analyse documentaire

La littérature scientifique regorge d'articles pertinents sur la société contemporaine de surveillance. Leur concours est capital : son émergence, ses mécanismes et son éventuelle existence sont autant d'éléments importants pour notre étude qu'ils sont abordés dans certaines contributions littéraires et scientifiques. Ainsi, « il serait à la fois absurde et présomptueux de croire que nous pouvons nous passer purement et simplement de ces apports, comme si nous étions en mesure de tout réinventer par nous-mêmes »⁴.

Cette littérature sur laquelle nous nous sommes appuyés est constituée d'ouvrages et d'essais scientifiques, de rapports adressés aux politiques publiques et de recherches évaluatives sur les pratiques de surveillance. Composée d'éléments hétéroclites, celle-ci provient des pays majoritairement anglo-saxons ainsi que, plus modérément, de la France et de la Belgique. Tous n'ont bien sûr pas la même importance. Parmi les textes analysés, certains occupent une place majeure dans cette étude : les écrits de David Lyon et le rapport présenté par la Surveillance Studies Network.

En définitive, cette analyse documentaire vise à recueillir une série d'informations sur la société de surveillance et ses diverses modalités dans le but de faire émerger une connaissance nécessaire et suffisante à propos de ce phénomène. Pour autant, cette méthode ne recouvre qu'imparfaitement notre sujet d'étude : peu de documentation a été trouvée sur le sujet de la traçabilité. C'est pourquoi, nous avons procédé complémentarément à la direction d'entretiens de recherche semi-directifs pour obtenir les données manquantes.

⁴ L. VAN CAMPENHOUDT & R. QUIVY, *op. cit.*, p. 42.

4.2. L'entretien de recherche semi-directif

L'entretien constitue la deuxième méthode de recueil des données mobilisée dans notre recherche, et dont le recours présente une réelle plus-value eu égard à l'absence de données relatives aux pratiques judiciaires de traçabilité numérique. Défini comme « un outil d'informations sur les entités sociales et un instrument d'exploration privilégié du vécu des acteurs sociaux », plusieurs motifs méthodologiques nous ont incités à mobiliser cette méthode particulière⁵.

Tout d'abord, seul l'entretien permet d'accéder à certaines connaissances subordonnées au savoir ou au souvenir de l'interlocuteur. La traçabilité des comportements humains constitue, dans le chef des acteurs concernés, une pratique sensible qui ne peut être rendue accessible à tout un chacun. Dès lors, si cette pratique est difficilement observable, elle peut toutefois être restituée oralement. En outre, l'entretien permet d'accéder aux représentations sociales des différents acteurs. Ces données, intéressantes sur le plan social, confortent l'adoption de l'entretien comme technique de recueil des données. Cette méthode permet donc la collecte de données tant sur les représentations des acteurs – normes et valeurs – que sur les pratiques sociales – actions et stratégies – de ces derniers.

Plus précisément, nous avons adopté la conduite d'entretien semi-directif. Ce type d'entretien consiste principalement à laisser « venir l'interviewé afin que celui-ci puisse parler ouvertement, dans les mots qu'il souhaite et dans l'ordre qui lui convient »⁶. L'entretien semi-directif présente plusieurs avantages. D'une part, il permet au chercheur de mener sagement l'interaction avec l'interviewé. Un cadre trop rigide entraînerait le risque de passer à côté d'informations ou de données qui ne peuvent être abordées par des questions trop précises. D'autre part, ce type d'entretien accorde également la possibilité de recadrer l'échange avec son interlocuteur si celui-ci s'écarte de la thématique donnée. Ainsi, nous avons veillé à prévoir un guide d'entretien abordant les questions et les thématiques générales qui devront être discutées pendant l'entretien. Notons enfin que nous avons procédé à l'enregistrement des entretiens et à la retranscription des propos tenus dont nous avons obtenu au préalable l'accord afin d'éviter toute « fuite de la connaissance ».

⁵ J. POUPART, « L'entretien de type qualitatif: considérations épistémologiques, théoriques et méthodologiques », In *La recherche qualitative. Enjeux épistémologiques et méthodologiques*, Montréal, Gaëtan Morin, 1997, p. 180.

⁶ L. VAN CAMPENHOUDT & R. QUIVY, *op. cit.*, p. 171.

Après ces considérations générales, il nous semble opportun d'apporter de plus amples précisions quant à certaines modalités précédant l'accomplissement des entretiens semi-directifs. Ainsi, nous faisons état de la structure adoptée pour cette méthode de récolte des données et des difficultés rencontrées dans le cadre de sa mise en œuvre.

4.2.1. La structure des entretiens

La conduite d'entretiens semi-directifs ne peut se réaliser en l'absence d'une structure propre mais souple de la part du chercheur. Pour organiser les données émises par nos interlocuteurs, il est donc nécessaire de prévoir au préalable un plan structurel et flexible dans la mise en œuvre de cette méthode. À cet effet, le guide d'entretien permet d'atteindre un tel objectif.

Les entretiens menés par nos soins ont plus particulièrement porté sur huit aspects : la définition générale de la traçabilité ; l'apport judiciaire de la téléphonie mobile et son fonctionnement en matière de traçabilité ; l'apport judiciaire de la carte bancaire et son fonctionnement en matière de traçabilité ; l'apport judiciaire de la base de données et son fonctionnement en matière de traçabilité ; le champ d'application de la traçabilité ; la fréquence d'utilisation de ces nouvelles technologies ; les avantages et les désavantages de ces nouvelles technologies. Par la mise en place de cette structure particulière, nous estimons avoir pleinement abordé les pratiques judiciaires de traçabilité numérique.

4.2.2. Les difficultés rencontrées

Après avoir pensé la conception générale de nos entretiens semi-directifs, deux principales difficultés sont advenues dans leur mise en pratique. La première se rapporte à l'obtention d'entrevues auprès des acteurs judiciaires. En effet, nous avons été confronté à de multiples fins de non-recevoir lorsque nous avons contacté certains juges d'instruction et fonctionnaires de police, arguant le secret professionnel auquel ils étaient soumis. Nous avons toutefois multiplié nos demandes pour parvenir finalement à nous entretenir avec six juges d'instruction et trois fonctionnaires de police. Pour pallier ce faible échantillonnage, nous avons également procédé à la conduite d'entretiens auprès d'autres acteurs – trois agents des cellules « coordination justice », un agent de l'Institut belge des services postaux et des télécommunications, un expert judiciaire ainsi que deux chercheurs universitaires – pouvant nous transmettre, comme expliqué à la section 3.1. de la page 7, des enseignements pertinents.

La seconde difficulté réside dans le refus de deux juges d'instruction et d'un fonctionnaire de police, parmi l'ensemble des personnes mentionnées au paragraphe précédent, d'enregistrer les déclarations tenues lors d'entretiens semi-directifs de recherche. La motivation d'un tel refus est identique à la première difficulté : le secret professionnel fut invoqué à l'encontre de l'enregistrement en considération de la sensibilité de certaines mesures en matière de traçabilité. Nous avons dès lors choisi de ne pas retranscrire *in extenso* les discours prononcés par ces acteurs en considération des exigences de précision que requiert un tel exercice. Pour autant, cela ne signifie pas leur exclusion totale de notre étude ; ceux-ci s'y intègrent assurément dans la conception générale de notre mémoire.

En dépit des difficultés rencontrées, nous avons néanmoins rencontré, de par la multiplication de la conduite d'entrevues, une réelle saturation empirique atteinte lors de notre dernier entretien de recherche. En effet, l'accumulation de nouvelles informations n'a guère apporté de véritables connaissances supplémentaires. Nous avons dès lors estimé qu'une augmentation du matériel empirique par la constitution d'entretiens supplémentaires ne se justifiait plus, entraînant, par conséquent, l'arrêt de la collecte de ces données.

5. L'analyse de l'information

Après avoir collecté une série de données par le recours à certaines méthodes, le chercheur procède finalement à l'étude approfondie de ces informations brutes. Cette étape constitue un passage obligé pour celui qui souhaite « constater si ces dernières correspondent bien aux hypothèses ou, en d'autres termes, si les résultats observés correspondent aux résultats attendus par hypothèse »⁷. La vérification empirique s'érige de la sorte comme un enjeu majeur d'une telle phase. Cette dernière est donc essentielle et mérite quelques commentaires approfondis sur l'analyse que nous avons effectuée dans le cadre de notre étude. Ainsi, nous abordons, tout d'abord, le modèle d'analyse adopté par nos soins dans la conception générale de ce mémoire. Ensuite, nous évoquons la principale méthode d'analyse de l'information mobilisée au sein de nos recherches.

5.1. Le modèle d'analyse

Notre étude se base sur un modèle d'analyse spécifique, celui de l'analyse déductive. La précision d'un tel choix est importante dans une recherche puisqu'elle détermine la trajectoire du « cheminement intellectuel » du travail et son point de départ.

Cette analyse déductive consiste, plus précisément, en la recherche de la vérification empirique d'hypothèses dérivées d'une théorie. Autrement dit, il s'agit de déterminer, à partir d'une hypothèse particulière, plusieurs concepts abstraits dont certains indicateurs peuvent rendre compte dans le réel afin de vérifier celle-ci pour « falsifier⁸ » la théorie de départ.

Qu'est-ce qu'une hypothèse ? Il s'agit, selon Van Campenhoudt et Quivy, d'une proposition qui anticipe une relation entre deux termes pouvant être des concepts ou des phénomènes⁹. Concrètement, nous sommes parvenus à l'hypothèse suivante : « l'usage des nouvelles technologies de l'information et de la communication contribue au développement de formes de surveillance par la police dans l'espace public ». À partir de celle-ci, nous pouvons dégager plusieurs concepts interconnectés. Nous en avons distingué trois : « nouvelles technologies », « développement » et « surveillance ».

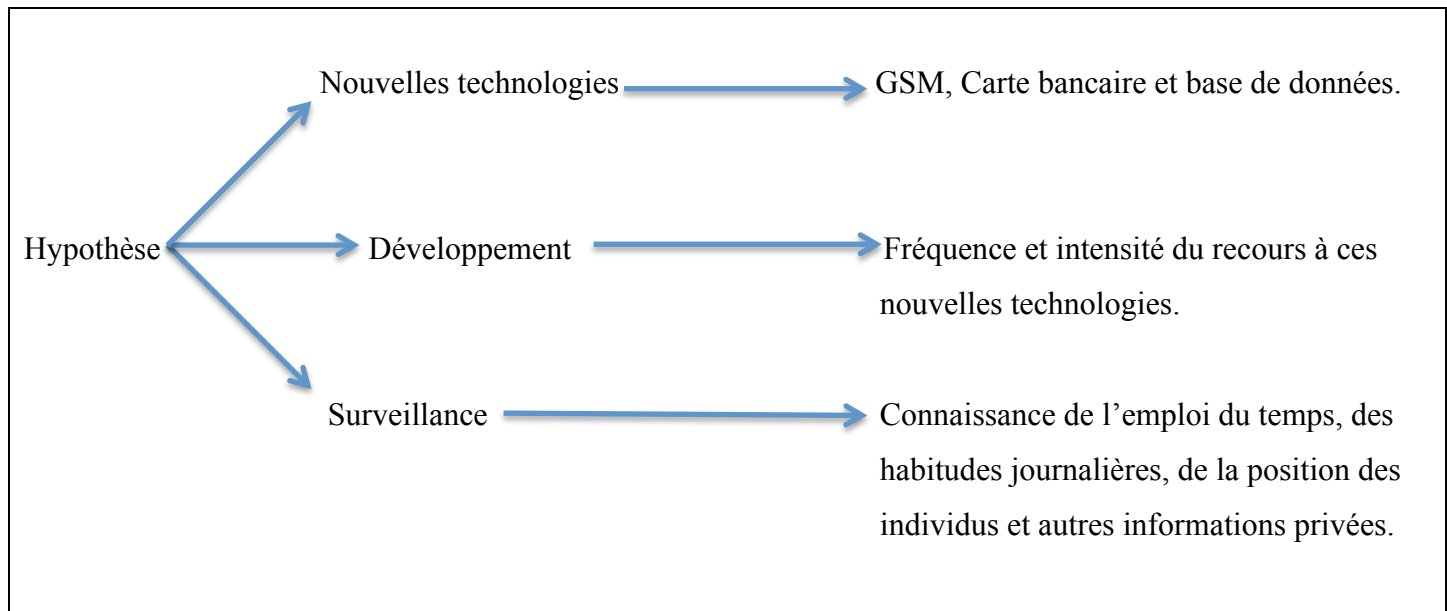
⁷ L. VAN CAMPENHOUDT & R. QUIVY, *op. cit.*, p. 187.

⁸ Terme emprunté à Karl Popper selon lequel un résultat de recherche n'est scientifique que s'il est falsifiable.

⁹ L. VAN CAMPENHOUDT & R. QUIVY, *op. cit.*, p. 128.

Enfin, il est question de déterminer des indicateurs afin de représenter ces notions abstraites dans la réalité concrète. Si ce principe est fort théorique, un simple cas suffit à rendre compte avec clarté des enjeux méthodologiques qui nous occupent ici. Prenons, par exemple, le concept de « nouvelles technologies ». Comment apprécier ou étudier une telle notion abstraite dans la réalité ? En tant que telle, nous ne pouvons l'observer sur le terrain de recherche. Toutefois, il existe des indicateurs qui permettent d'étudier un tel concept. Ce n'est qu'en étudiant, par exemple, le GSM, son fonctionnement et ses mécanismes que nous pourrions nous représenter concrètement le concept de « nouvelles technologies ».

L'ensemble des indicateurs se retrouve dans le cadre ci-dessous. Le « tracé » adopté dans nos recherches se présente sous cette forme précise :



5.2. La méthode d'analyse de l'information

Au sein de ce modèle général, s'intègrent *in fine* un certain nombre de méthodes d'analyse de l'information réparties en deux grandes catégories : l'analyse statistique des données et l'analyse de contenu. Nous avons opté pour cette dernière. Nous en explicitons le choix dans cette dernière section.

Couramment utilisée, l'analyse de contenu présente l'avantage de pouvoir offrir « la possibilité de traiter de manière méthodique des informations et des témoignages qui présentent un certain degré de profondeur et de complexité, comme, par exemple, les rapports

d'entretiens semi-directifs »¹⁰. Considérée par Luc Van Campenhoudt et Raymond Quivy comme « meilleure que toute autre méthode de travail », elle permet de satisfaire les diverses exigences méthodologiques lorsque le chercheur est confronté à des matériaux riches et complexes¹¹. Plus précisément, nous avons opté pour une analyse thématique de contenu des données préalablement recueillies. Un tel choix s'explique par la volonté de « mettre en évidence les représentations sociales ou les jugements des locuteurs à partir d'un examen de certains éléments constitutifs du discours »¹². Mû par la volonté de souligner les similitudes et les contradictions, de déterminer l'importance des principes généraux perçus au travers des discours multiples et de les organiser rationnellement, la décision de recourir à l'analyse thématique de contenu s'imposait naturellement.

¹⁰ L. VAN CAMPENHOUDT & R. QUIVY, *op. cit.*, p. 207.

¹¹ *Ibidem.*

¹² *Ibid.*, p. 208.

Deuxième partie :
Émergence de la Société de Surveillance

1. Introduction

« *Le soupçon et la peur sont de bons surveillants* »
- Proverbe français ; *Recueil d'apophtegmes et axiomes* (1855)

La surveillance n'est pas un phénomène nouveau, loin s'en faut. Elle accompagne l'humanité depuis l'aube des civilisations. En témoigne *L'art de la guerre* du stratège et fin observateur chinois Sun Tzu qui décrit, aux alentours du VI^e siècle avant J.-C., la manière dont un espion s'infiltrait pour observer l'ennemi.

Dans les sociétés anciennes, la surveillance était liée aux relations d'interconnaissance, de parenté ou de voisinage et était immanente aux rapports sociaux. Elle était diffuse, permanente et atmosphérique, mais ne participait d'aucun système formel et organisé¹³. Plutôt corbeau de village que *Big Brother*, donc. Ce n'est qu'au XVII^e siècle que la mise en place d'administrations centralisées et le développement des règles de bureaucratie vont permettre de normaliser et pérenniser la surveillance. Cette même époque vit l'essor des méthodes cartésiennes, rationalistes et leurs applications aux pratiques organisationnelles. Ainsi, la collecte et la conservation d'informations par écrit ont permis de se détacher progressivement des réseaux et contrôles sociaux informels au profit d'une organisation standardisée.

L'essor de l'informatisation et du numérique vient considérablement transformer la surveillance telle qu'elle avait été imaginée lors de cette époque de bureaucratisation par Bentham et son panoptique¹⁴. L'évolution des technologies donne aux États des potentialités accrues et quasiment instantanées, permettant d'étendre indistinctement la surveillance sans délimiter précisément et ponctuellement ses cibles¹⁵. Ainsi, McCahill et Norris ont approximativement estimé à 4.2 millions le nombre de caméras de vidéosurveillance en Grande-Bretagne. « Il y est donc virtuellement impossible de traverser des espaces publics sans être photographié et sans voir son image enregistrée »¹⁶. Une surveillance à large spectre dotée d'une « mémoire informatique » par le biais de différentes bases de données incite *grosso modo* de nombreux auteurs à souligner l'apparition d'une « société de surveillance ».

¹³ C. LAVAL, « Surveiller et prévenir. La nouvelle société panoptique », *Revue du MAUSS*, 2012, vol.2, p. 69.

¹⁴ Le panoptique est une structure architecturale permettant à un gardien, logé dans une tour centrale, d'observer tous les prisonniers enfermés dans des cellules individuelles autour de la tour, sans que ceux-ci puissent savoir s'ils sont observés.

¹⁵ I. JABLONKA, « Aux origines de la surveillance de masse. Entretien avec Sophie Cœuré », In *La Vie des idées*, 12 janvier 2016.

¹⁶ C. NORRIS & G. ARMSTRONG, *The Maximum Surveillance Society – The Rise of CCTV*, Oxford et New York, Berg, 1999, p. 3.

Pour autant, préalablement à l'étude approfondie de ce qu'est la société contemporaine de surveillance généralisée, nous estimons opportun d'effectuer un détour auprès des différents facteurs généraux ayant rendu possible l'apparition d'une telle société. En effet, il est particulièrement intéressant d'aborder les évolutions sous-jacentes d'un phénomène pour en comprendre ses tendances contemporaines. Le passé récent conditionne le présent. Dans le chapitre suivant, nous abordons plusieurs facteurs ayant, à la lecture de plusieurs auteurs mentionnés au fil de nos développements, permis l'émergence de la société de surveillance.

2. Les facteurs d'émergence de la Société de Surveillance

La société de surveillance est un phénomène dont l'apparition contemporaine repose sur une assise immatérielle. Son avènement s'appuie ainsi sur plusieurs tendances latentes formant un certain nombre de facteurs actuels ou passés, épars et hétéroclites ! De tels facteurs sont incontestablement de natures différentes. Pris un à un, ils n'ont que très peu de points communs. Toutefois, leur conjugaison aboutit à un résultat identique : l'intensification des pratiques de surveillance. Autrement dit, c'est l'addition d'un tel ensemble disparate de facteurs qui permet d'aboutir à l'émergence d'une société de surveillance.

Quels sont ces facteurs ? Nous analysons dans les sections suivantes cinq facteurs ayant permis le développement d'une surveillance diffuse : la volonté de supprimer le risque, l'obsession sécuritaire, l'influence du domaine militaire, l'économie politique de la surveillance et l'économie d'informations personnelles.

2.1. Le risque, objet d'une attention grandissante dans la société contemporaine

La notion de « risque » s'est immiscée dans l'action des gouvernements occidentaux au milieu du XIX^e siècle¹⁷. Plus précisément, l'obsession sociétale pour ce concept trouve son origine dans les changements, socio-économiques et politiques, inhérents aux transformations de la société, passant d'une société pré-moderne à une société post-moderne¹⁸. Ainsi, avec l'avènement de l'ère industrielle, de nombreux accidents émaillèrent notamment l'histoire de nos contrées occidentales. De Tchernobyl en passant par Fukushima, les exemples ne manquent pas. « Quand les désastres – de masse ou individuels – sont devenus une priorité auprès des acteurs politiques, un ensemble très différent de représentations et de techniques de traitement du risque, signalé par des termes comme *sécurité*, *précaution* et *sûreté*, s'est imposé »¹⁹. C'est donc à partir de ces multiples changements sociaux que peut être observé le développement d'un sentiment patent d'insécurité dont la conséquence est assurément une attention grandissante à la notion de risque²⁰.

¹⁷ P. PERETTI-WATEL, *Sociologie du risque*, Paris, Armand Colin, 2000, p. 48.

¹⁸ D. LUPTON, *Risk*, 2^e éd., Londres, Routledge, 2003, p. 13.

¹⁹ J. SIMON, « Le parti du risque », *Vacarme*, 2007, vol. 3, p. 17.

²⁰ D. NEYLAND & I. KROENER, « New technologies, security and surveillance », In *The routledge handbook of surveillance studies*, éd. par Kirstie Ball, Kevin D. Haggerty & David Lyon, Abingdon, Routledge, 2012, p. 143.

Si le domaine industriel est particulièrement sensible à cet impératif du risque zéro, nous retrouvons une exigence semblable en matière de délinquance et de criminalité. Dans ce cadre, le risque désigne l'action potentiellement néfaste, contrôlable et calculable par toute une série de dispositifs et de mesures de surveillance, d'un ensemble de personnes ou de situations. Il ne pourrait être considéré comme tel si la menace ou le péril est incalculable, empêchant ainsi la mise en place de mesures préventives. C'est ce que confirme Vincent Francis, professeur à l'Université catholique de Louvain-la-Neuve et spécialisé dans les questions de sécurité et de surveillance, lorsqu'il affirme dans un entretien qu'« *un dispositif de sécurité s'attaque à un risque en tant qu'il est calculable et dont on peut prévoir la probabilité de survenue* »²¹. Un événement considéré comme menaçant pour la société doit donc pouvoir être apprécié avant sa survenance dans le but de le supprimer.

Au sein de cette appréciation préventive, les instruments de surveillance jouent un rôle considérable. De nombreux développements dans les technologies de surveillance ont en effet pour assise l'évaluation de ce risque, la gestion et l'écartement de celui-ci. Ils emportent avec eux le postulat selon lequel les risques et problèmes peuvent être résolus²². Le recours à la caméra de vidéosurveillance est ainsi mu par un fantasme de tout voir pour tout contrôler. De plus en plus de données et d'informations personnelles sont captées et fichées « au cas où ». Idéalement, il s'agirait de pouvoir prévenir toute action suspecte par le recours toujours plus contraignant à des mesures de surveillance de plus en plus généralisées²³.

La logique dans la poursuite et la répression des crimes et délits est devenue beaucoup plus préventive. De plus, « l'utilisation de l'exploitation des données et du profilage visant l'identification d'une situation à risque oriente les pratiques de la surveillance vers l'examen des actions et des transactions de la population en général »²⁴ ! Cet examen permet alors de cibler des interventions mises en place pour des individus ou des groupes d'individus dont la société considère qu'ils sont vulnérables ou qu'ils peuvent, à tort ou à raison, entraîner un risque envers autrui²⁵. On justifie par conséquent le développement croissant des mesures de surveillance de la population au motif d'écarter *a priori* des comportements et actions considérés comme potentiellement dangereux.

²¹ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²² D. NEYLAND & I. KROENER, *op. cit.*, p. 143.

²³ G. BERTHOUD, « L'horizon d'une surveillance omniprésente ? », *Revue européenne des sciences sociales*, 2002, p. 164.

²⁴ SURVEILLANCE STUDIES NETWORK, *A Report on the Surveillance Society*, Knowledge House (Mark Siddoway), 2006, p. 11.

²⁵ *Ibidem*.

Outre la justice pénale et sa gestion de plus en plus préventive de la criminalité, plusieurs exemples illustrent la tendance générale à l'évaluation du risque et à sa prévention au sein de questions pluridisciplinaires. Celle-ci est particulièrement flagrante en matière de contrôle des frontières et de sécurité des transports aériens. Le programme CAPPS II²⁶, par exemple, autorise l'accès pour les organes de gestion de la sécurité des compagnies aériennes aux données personnelles des voyageurs dans le but d'évaluer la menace et le risque qu'ils constituent pour la sécurité. Chaque passager est étiqueté en fonction du danger qu'il représente et peut se voir refuser, en fonction de cette évaluation du risque, l'entrée dans l'avion. Le secteur commercial n'échappe pas non plus à cette tendance. De grandes entreprises ont de plus en plus souvent recours à l'estimation de la valeur relative des consommateurs individuels par l'usage et le recoupement de plusieurs bases de données. L'objectif est de pouvoir évaluer et répartir au mieux les différents coûts d'investissement réalisés par ces sociétés.

« Cette surveillance par anticipation devrait permettre des relations sociales moins incertaines, moins imprévisibles, ou encore moins risquées dans un monde où la confiance est particulièrement fragile »²⁷. Cette volonté d'éliminer à tout prix le risque laisse perplexe. Pouvons-nous considérer que nous vivons dans un monde plus dangereux qu'auparavant ? Si la réponse est, à notre avis, négative, il n'en demeure pas moins que le risque est désormais bien plus qu'une menace : il est devenu un moteur de l'action publique en matière de surveillance²⁸.

2.2. L'obsession sécuritaire à la suite d'événements catalyseurs

Comme évoqué précédemment, la théorie du risque mobilise un nombre toujours plus important d'instruments de surveillance dans le but de prévenir la commission d'une infraction. Toutefois, le risque zéro n'existe pas, n'a jamais existé et n'existera jamais. Il s'agit d'une illusion dangereusement liberticide dans laquelle se bercent, et bercent la population, nos responsables politiques. De nombreux faits, plus ou moins graves, parviennent ainsi à traverser les mailles d'une surveillance accrue par cette volonté de tout anticiper.

²⁶ Computer Assisted Passenger Pre-screening System II.

²⁷ G. BERTHOUD, *op. cit.*, p. 164.

²⁸ U. BECK, *La société du risque : sur la voie d'une autre modernité*, Paris, Aubier, 2002.

La conjoncture d'un début de XXI^e siècle mouvementé vient également exacerber les tendances vers une surveillance à tout-va. Le contexte des attaques terroristes du 11 septembre 2001 a notamment joué un rôle essentiel dans l'intensification des pratiques de surveillance légitimée par le spectre insaisissable des menaces²⁹. Un sentiment d'insécurité général dans l'ensemble du monde occidental a favorisé certaines décisions et l'adoption de certaines mesures législatives³⁰. Cette vague sécuritaire, découlant d'un contexte d'insécurité, a plus particulièrement engendré une demande pressante tant de la part des autorités étatiques que de l'opinion publique pour un renforcement des opérations de surveillance et des moyens pour y parvenir³¹. Notons qu'une telle vague se caractérise de deux façons. Elle est tout d'abord normative dans le sens où ce mouvement se traduit par la création ou l'extension de nombreux fichiers et la mise en place de nouveaux moyens d'investigation en faveur de la police³². Cette vague sécuritaire est ensuite technologique dès lors qu'elle repose, selon Alex Türk, sur le mythe du contrôle absolu des individus par des outils numériques³³.

Toute période marquée par la survenance d'actes terroristes, ou tout autre acte générant un sentiment de crainte diffus, s'accompagne ainsi d'une forte tendance à accepter un renforcement du contrôle et de la surveillance dans l'espoir de préserver la sécurité individuelle et collective³⁴. L'action politique est bien souvent influencée par les soubresauts de l'actualité et les pressions populaires qui en découlent. Aux États-Unis, le « USA Patriot Act » a été voté par le Congrès américain le 26 octobre 2001 afin de renforcer les pouvoirs des agences gouvernementales dans la lutte contre le terrorisme. Adoptée quelques semaines après les attentats du 11 septembre, cette loi augmente considérablement les mesures de surveillance. Elle autorise notamment les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans obtenir au préalable le consentement des utilisateurs qui ne seront pas informés de telles démarches.

²⁹ É. SADIN, *Surveillance globale : enquête sur les nouvelles formes de contrôle*, Paris, Climats, 2009, p. 184.

³⁰ G. BERTHOUD, *op. cit.*, p. 160.

³¹ A. TÜRK & P. PIAZZA, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Culture & Conflits*, 2009, p. 124.

³² *Ibidem* ; Le gouvernement français a notamment milité pour l'adoption d'un Passenger Name Record (PNR) européen à la suite des attentats de Charlie Hebdo. Ce projet vise à fichier toutes les données personnelles concernant les détails d'un voyage de l'ensemble des passagers européens. Il a récemment été adopté au même titre que le recours par les services de renseignements français à l'IMSI-catcher, instrument technologique permettant une interception plus aisée du trafic de téléphonie mobile. *Voy. Point* 3.1.1.3. p. 48.

³³ A. TÜRK & P. PIAZZA, *op. cit.*, p. 124.

³⁴ A noter que si la plupart des auteurs ont recours à cet exemple du terrorisme, c'est en raison de l'essence même de cette infraction particulière : l'emploi de la terreur à des fins politiques, religieuses ou idéologiques. D'autres actes délictueux peuvent également produire une crainte généralisée justifiant l'adoption de mesures de surveillance. Par exemple : la pédopornographie et la cyber délinquance.

En Europe, les principaux gouvernements emboîtèrent le pas à l'Amérique. Du « Terrorism Act » au Royaume-Uni à la « Loi renseignement » en France, en passant par la « Ley de Seguridad Ciudadana » en Espagne, de nombreuses mesures législatives furent adoptées en réaction aux différents événements traumatisants de terrorisme³⁵. Dans cette optique, ces textes de loi visent à renforcer le cadre juridique des activités de renseignement par l'adoption de mesures controversées en matière de surveillance et de lutte contre le terrorisme.

Cette intensification des dispositifs de surveillance est toutefois loin d'être une nouveauté ! Ce phénomène particulier exprime surtout une accélération d'un mouvement engagé de longue date³⁶. Il serait erroné de croire en l'absence de dispositifs organisés et rationnels de surveillance avant la survenance de ces attaques terroristes. Le système d'interception de certaines télécommunications mis en place lors de la seconde guerre mondiale, dénommé Échelon, en est le parfait exemple³⁷. En 1954, le sociologue français Jacques Ellul dénonçait en outre le principe selon lequel « pour être certain d'attraper des criminels, il faut que chacun soit surveillé, que l'on sache ce que fait chaque citoyen, ses relations, ses habitudes, ses distractions. Et l'on est de plus en plus en mesure de le savoir »³⁸. Nous pouvons donc affirmer que si le contexte du 11 septembre n'a pas créé de toutes pièces une surveillance généralisée, il a permis toutefois de révéler et de renforcer certaines pratiques occultes déjà existantes³⁹. Plus particulièrement, les mesures de surveillance adoptées en riposte aux attentats témoignent de la place centrale qu'occupe insidieusement la technologie comme réponse aux problèmes du monde moderne⁴⁰.

En définitive, l'événement, aussi tragique soit-il, est un prisme au travers duquel nous pouvons contempler le changement social structurel en cours⁴¹. À l'instar de la théorie du risque, le contexte influence la manière de gérer et de contrôler un groupe d'individus donné. Tout acte traumatisant est ainsi révélateur d'une réelle intensification *a posteriori* des pratiques de surveillance et du recours à divers instruments technologiques sur lesquels elles se basent pour en prévenir une nouvelle survenance.

³⁵ I. RAMONET, *op. cit.*, p. 115.

³⁶ D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », *op. cit.*, p. 90.

³⁷ Échelon est un programme destiné à l'interception de télécommunications privées et publiques mis en place durant la seconde guerre mondiale, bien avant les attentats du 11 septembre...

³⁸ J. ELLUL, *La Technique ou l'Enjeu du siècle*, Economica, Paris, 1990, p. 92.

³⁹ G. BERTHOUD, *op. cit.*, p. 162.

⁴⁰ *Ibidem*.

⁴¹ D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », *op. cit.*, p. 93.

2.3. La militarisation de la surveillance

L'influence du domaine militaire est loin d'être anodine. Si la théorie du risque et l'influence du contexte viennent intensifier les pratiques de surveillance déjà existantes, encore faut-il pouvoir disposer du support technologique adéquat. Cette sphère particulière offre ainsi une base matérielle déterminante pour le développement et l'intensification des pratiques de surveillance liées aux nouvelles technologies. Dans ce cadre-là, le domaine militaire oriente considérablement la surveillance actuelle.

Avant toute chose, le concept de « militarisation » sous-entend qu'une autre institution ou sphère sociale assume le transfert de certaines caractéristiques propres aux forces armées⁴². Pour comprendre ce processus, il est donc nécessaire de mettre en lumière ces attributs particuliers. Selon Kevin Haggerty et Richard Ericson, le trait distinctif de l'armée contemporaine est son utilisation massive des technologies de pointe issues notamment de la guerre froide et de la course effrénée à l'armement⁴³. Par conséquent, la militarisation désigne la transmission nécessaire de ces ressources technologiques à divers autres domaines institutionnels tels que la justice pénale ou la sécurité publique pour la réalisation de leurs objectifs propres. Ces technologies militaires s'implantent ainsi dans le paysage de la surveillance. Un tel transfert n'est toutefois pas automatique. Il peut, d'une part, résulter de « l'action dirigée » de l'État qui souhaite les inscrire volontairement dans différents domaines institutionnels. D'autre part, les technologies peuvent « s'infiltrer » dans la société grâce aux efforts des entreprises qui les ont produites et développées⁴⁴.

Nous pouvons donc clairement constater l'apparition, dans le domaine de la justice pénale, de technologies électroniques qui concourent à la production de l'information numérique et qui ont été originellement développées dans un contexte militaire⁴⁵. L'ordinateur est un premier exemple de technologie dont la genèse a été intimement liée aux intérêts militaires. Pensé à l'origine comme une machine permettant de décoder les transmissions cryptées lors de la seconde guerre mondiale, son évolution et son informatisation offrent de nombreuses

⁴² K. HAGGERTY & R. ERICSON, « Les technostructures militaires du maintien de l'ordre », In *La militarisation des appareils policiers*, sous la dir. de Frédéric Lemieux et Benoît Dupont, Lévis, Les Presses de l'Université Laval, 2005, p. 112.

⁴³ *Ibid.*, p. 113.

⁴⁴ K. HAGGERTY & R. ERICSON, *op. cit.*, p. 114.

⁴⁵ C. DANDEKER, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge, Polity press, 1990, p. 45.

possibilités de surveillance. La création de bases de données numériques et de fichiers personnels permet ainsi, tant pour les services de police que pour les entreprises privées, l'avènement d'une « data surveillance ». Les systèmes de positionnement géographique (GPS) et le développement de l'Internet sont également deux autres illustrations contemporaines de technologies conçues à partir de capacités militaires intégrées. L'histoire moderne de la surveillance et de son intensification peut donc être tracée depuis les premiers développements technologiques issus de la seconde guerre mondiale, dont l'objectif était de faire de la planète un espace totalement défendable et sécurisé⁴⁶.

Cette tendance est loin de s'estomper. En mai 2007, les premiers drones, de petits appareils militaires sans pilote, équipés d'une caméra de vidéosurveillance ont commencé à survoler la ville de Liverpool. Originellement conçues pour la reconnaissance militaire, la police de Merseyside use désormais de ces « caméras volantes » pour surveiller les désordres publics, les foules, voire les embouteillages⁴⁷. Il en va de même à Paris où la préfecture de police vient de lancer un appel d'offres en vue de mettre à sa disposition des drones destinés à des missions d'observation et de surveillance⁴⁸.

L'influence du secteur militaire ne se limite pas au domaine des nouvelles technologies de surveillance. Son incidence est telle qu'elle procède à la militarisation de la société et de sa sécurité. Le vocabulaire quotidien en est envahi. François Hollande déclarait, au lendemain des attentats terroristes du 13 novembre 2015, que : « *La France est en guerre. Les actes commis vendredi soir sont des actes de guerre [...]. Ils sont le fait d'une armée djihadiste.* »⁴⁹. À l'échelle plus locale, il est également courant d'encourager la lutte contre la drogue et la criminalité. Cette impulsion guerrière s'étend jusque dans le monde des affaires, où la « guerre des données personnelles » est sortie de la pénombre des stratégies commerciales⁵⁰. « Les capacités de défense militaire et le concept de contrôle sont devenus des parties dominantes de l'aménagement urbain »⁵¹. La surveillance n'échappe guère à cette tendance.

⁴⁶ SURVEILLANCE STUDIES NETWORK, *op. cit.*, pp. 13-14.

⁴⁷ J. ORR, « Police send 'spy drone' into the skies », *The Guardian*, mis en ligne le 21 mai 2007, consulté le 28 mars 2016. Disponible sur : <http://www.guardian.co.uk/crime/article/0,,2084801,00.html>.

⁴⁸ J.-M. NORMAND, « Bientôt des drones de surveillance pour la préfecture de police », *Le Monde*, mis en ligne et consulté le 21 mars 2016. Disponible sur : <http://drones.blog.lemonde.fr/2016/03/31/la-prefecture-de-police-commande-des-drones-de-surveillance/>.

⁴⁹ <http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-devant-le-parlement-reuni-en-congres-3/>, consulté le 17 février 2016.

⁵⁰ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 14.

⁵¹ *Ibidem*.

2.4. L'économie politique de la surveillance

La surveillance est, d'un point de vue lucratif, un marché extrêmement important. En raison de l'essor des ordinateurs et des bases de données dans la collecte d'informations, les technologies de surveillance sont en train de devenir l'un des commerces les plus rentables pour les entreprises actives dans le nouveau « business de l'anti-terrorisme »⁵². Pouvons-nous dès lors parler de privatisation commerciale en pleine expansion d'une surveillance accrue ?

« Il y a clairement l'implication du privé d'une manière générale dans l'émergence des nouvelles technologies de surveillance, mais on constate surtout l'apparition d'un marché très important », confirme Vincent Francis⁵³. Entamé aux États-Unis depuis le début des années 1970, un processus de privatisation de la sécurité et de la surveillance est actuellement en pleine expansion. En Europe, il faut attendre la chute du mur de Berlin en 1989 pour observer cette tendance. Comment expliquer un tel mouvement ? Selon Vincent Francis, *« l'industrie militaire a dû se recycler et trouver de nouveaux clients, la menace militaire étant fortement amoindrie. Il a fallu inonder le marché privé de nouvelles technologies »*⁵⁴.

Issu de ce processus, un véritable secteur privé de « l'industrie de la sécurité et de la surveillance » a ainsi vu le jour. Il regroupe en son sein de nouvelles entreprises liées aux hautes technologies ainsi que les sociétés de sécurité traditionnelles et les grands fournisseurs militaires⁵⁵. Notons que l'influence du domaine militaire est également considérable dans ce mouvement vers une privatisation de plus en plus importante de la surveillance. Plusieurs nouvelles sociétés de haute technologie provenant de cette industrie particulière permettent l'infiltration sur le marché civil de produits de surveillance dont le « caractère militaire » n'est pas négligeable⁵⁶. TRW, par exemple, anciennement partenaire de la société américaine chargée des contrats de défense, est actuellement l'un des leaders mondiaux en biométrie civile. La société française Sagem, dont le chiffre d'affaire s'élève à 1,275 milliards d'euros, fabrique quant à elle des produits allant des téléphones mobiles à des algorithmes de surveillance, en passant par des systèmes de reconnaissance aérienne automatisés⁵⁷.

⁵² J. STANLEY, *The Surveillance-Industrial Complex: How the American Government is conscripting businesses and individuals in the construction of a Surveillance Society*, Washington DC, ACLU, 2004, p. 27.

⁵³ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

⁵⁴ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

⁵⁵ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 15.

⁵⁶ *Voy.* Section 2.3. p. 24.

⁵⁷ <http://www.sagem.com/fr/societe>, consulté le 23 février 2016.

Ces diverses entreprises de l'industrie de la surveillance ont un intérêt prononcé pour le développement de politiques sécuritaires, et encouragent l'intensification de ces dernières auprès des pouvoirs publics. Des groupes d'intérêts se forment ainsi au sein de cette industrie dans le but de promouvoir leurs produits. Ainsi, l'Union Américaine des Libertés Civiles soutient l'idée, par certains e-mails obtenus dans leurs recherches, que les responsables aéroportuaires recevaient déjà des sollicitations de la part de certaines entreprises actives dans les technologies de surveillance peu de temps après les attentats du 11 septembre⁵⁸. Même si ces activités lobbyistes ne sont que trop rarement exposées au grand jour, Vincent Francis tend à confirmer leur existence : « *Il faut les vendre et faire tourner la machine. Il y a clairement une pression de ce côté-là avec notamment les attentats du 11 septembre.* »⁵⁹.

D'autres entreprises et sociétés du secteur privé dont l'essence n'est toutefois pas sécuritaire peuvent également être amenées à influencer cette croissance exponentielle de la surveillance « industrialisée ». Nous pensons notamment au développement des entreprises de télécommunication, des banques et assurances dont le rôle clé dans ce domaine ne peut être omis. Le gouvernement belge, par exemple, tend à contraindre de plus en plus ces organisations privées, pour des raisons d'intérêt public, à respecter des obligations en matière de collecte, de conservation et de communication de données qui dépassent le cadre des activités « naturelles » de ces entreprises. Désormais, les établissements financiers, les opérateurs de téléphonie et toute autre société commerciale sont associés à des processus de traitements de données par le biais de normes légales imposant leur collaboration avec les autorités étatiques et judiciaires.

En conclusion, le domaine industriel de la sécurité et de la surveillance est en constante expansion ces dernières années. Selon les chiffres du cabinet américain Security Stock Watch, la croissance de cette industrie dans son ensemble a régulièrement dépassé l'indice du Dow Jones et les valeurs de haute technologie du NASDAQ⁶⁰. Nous sommes ainsi confrontés à un étrange paradigme où l'émergence et le développement d'un secteur privé gravitant autour de la surveillance, poussé par les avantages qu'il en retire, contribuent activement à renforcer et à intensifier cette même surveillance par son apport en moyens techniques permettant à celle-ci de s'étendre et d'agir de manière toujours plus efficace.

⁵⁸ J. STANLEY, *op. cit.*, p. 28.

⁵⁹ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

⁶⁰ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 15.

2.5. Les économies de l'information personnelle

La surveillance n'est pas uniquement conduite par l'état et les entreprises. Elle peut également l'être par la population ordinaire⁶¹. Après les attentats de Londres du 7 juillet 2005, tant les chaînes de télévisions que la police encouragèrent les citoyens à utiliser la caméra de leur smartphone pour filmer des individus au comportement suspect⁶². En outre, depuis mai 2006, les riverains de Shoreditch, un quartier de la capitale anglaise, peuvent regarder une chaîne de télévision diffusant en permanence les images des caméras de vidéosurveillance locales. Ils sont de la sorte priés de signaler tout comportement inapproprié à la police⁶³. En Belgique, le concept du « réseau d'information de quartier » procède de la même logique. Association structurée entre les citoyens et la police locale, un tel réseau consiste en la surveillance de tout fait suspect dans un quartier par ses habitants. De ces illustrations se dégage nettement un dernier facteur contemporain et fondamental : celle d'une démocratisation de la surveillance, auprès de monsieur Tout-le-Monde, rendue possible par la disponibilité de technologies d'observation dont le principal effet est de brouiller la distinction entre ceux qui observent et ceux qui sont surveillés⁶⁴.

Certes, ces méthodes ne s'éloignent guère des pratiques traditionnelles de surveillance de ses voisins que l'on observe à travers les rideaux. Toutefois, celle-ci est plus intensive que jamais. Quoi de mieux pour les services de police qui souhaitent élargir leur surveillance que d'associer les citoyens dans une telle tâche ? Outre l'efficacité d'une telle mesure, c'est l'essence même de ses pratiques qui se retrouve au centre des critiques. Le citoyen est devenu un acteur dynamique et actif de sa propre surveillance.

Et ce n'est pas tout ! Un nombre toujours croissant d'individus exposent leur vie privée à la vue et au su de tous sur les réseaux sociaux. À cet égard, Stéphane Leman-Langlois, professeur à l'Université Laval du Québec et spécialisé dans les questions de sécurité et de surveillance, estime dans un entretien réalisé dans le cadre de nos recherches « *qu'à de multiples niveaux bénins, nous nous observons et nous donnons à l'observation sur de*

⁶¹ Cette surveillance par les individus est également abordée, sous un autre angle, à la sous-section 2.2.1. p. 36 relative aux « confusions à éluder ».

⁶² SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 15.

⁶³ A. IGGULDEN, « CCTV channel beamed to your home », *The Telegraph*, mis en ligne le 10 mai 2006, consulté le 29 mars 2016. Disponible sur : <http://www.telegraph.co.uk/news/uknews/1517836/CCTV-channel-beamed-to-your-home.html>.

⁶⁴ B. DUPONT, « Hacking the Panopticon: distributed online surveillance and resistance », In *Surveillance and governance: Sociology of Crime Law and Deviance*, éd. par Mathieu Deflem, Bingley, Emerald, 2008, p. 33.

multiples plateformes numériques qui fonctionnent à l' à quoi pensez-vous, aux nouvelles de soi-même, aux selfies et autres gracieux dons de notre information personnelle la plus intime »⁶⁵. L'exemple des réseaux sociaux illustre ainsi parfaitement une nouvelle tendance, bien plus pernicieuse que la première explicitée ci-dessus, de surveillance par les différents individus. Que nous le voulions ou non, nous exposons de plus en plus inconsciemment sur le devant de la scène notre vie privée. Du téléphone portable à la carte bancaire, du fichage génétique à la carte de transport, du suivi des connexions internet à la multiplication des caméras de vidéosurveillance, nous produisons sans cesse une quantité gargantuesque d'informations. Nous multiplions ainsi, par fatalisme, par ignorance ou par lassitude, les traces qui vont permettre de nous surveiller ou de nous tracer, de savoir ce que nous avons fait, où et avec qui. Tant de manière active que passive, le citoyen encourage par conséquent l'intensification de sa propre surveillance.

⁶⁵ Entretien avec Monsieur Stéphane Leman-Langlois réalisé le 25 mai 2016.

3. Conclusion

Depuis les temps les plus reculés où l'homme devint homme et fut doté de vue et de raison, il regarde son voisin : mû par l'instinct de survie, il mesure ses gestes, cherche à deviner ses intentions, analyse et anticipe. Un rapport naturel et nécessaire à sa protection s'établit entre lui et l'extérieur, où une certaine mesure de crainte et de suspicion trouve sa juste place.

Quand les hommes se rassemblent pour se constituer en société, ces regards, plutôt que de se cumuler, tendent à s'abstraire pour former une masse qui se matérialise dans la fonction : la surveillance devient un rôle social, par exemple par le biais de l'espionnage, dans les anciennes civilisations guerrières. L'optique est alors de protéger le groupe, d'assurer la sécurité d'un ensemble de personnes de manière efficace. Dans ce même ordre d'idées vient s'inscrire la bureaucratisation de la surveillance, la naissance de la collecte d'informations et sa modernisation explosive au cours du siècle dernier.

Une série de faits sociaux viennent concomitamment se greffer sur cette évolution, participent à son essor et le modulent : un besoin de protection accru dans la masse informe – et lunatique – de l'opinion publique contre un risque diffus et des événements néfastes ; une application répandue des technologies opérationnelles militaires à la société civile ; l'avènement d'un secteur privé qui participe activement au développement technologique en étroite collaboration avec les États et les particuliers ; l'intégration, enfin, de ces mêmes particuliers dans le processus de surveillance, avec pour ultime récompense l'assurance de la sécurité. La surveillance – par le biais de tous ces facteurs – se développe ainsi dans le contexte de la modernité.

Le phénomène, son avènement et son accélération, ne sont pas axiologiquement *mauvais* : un bon outil est un outil efficace, nonobstant l'usage qu'on en fait. Néanmoins, ils présentent des risques. Pouvons-nous ignorer le risque que certaines catégories sociales ou ethniques fassent l'objet d'une surveillance accrue et discriminatoire ? Pouvons-nous ignorer les conséquences nuisibles que de telles pratiques sont susceptibles d'avoir ? Et cette situation n'est-elle pas déjà présente à l'intérieur de nos sociétés ? Ces questions méritent d'être posées dans ce mémoire dont les développements subséquents apportent implicitement certains éléments de réponse.

Troisième partie :
Étude de la Société de Surveillance ou
la « surveillance surveillée »

1. Introduction

*« Je ne crois pas que le genre de société que je décris arrivera,
mais je crois que quelque chose qui y ressemble pourrait arriver »*
- George Orwell

Toute entreprise scientifique consiste à analyser le réel pour mieux le comprendre. Le concept de « société de surveillance » s'est lentement répandu dans les sciences sociales et la criminologie pour devenir depuis une dizaine d'années un incontournable centre d'attention des cercles académiques anglo-saxons. La présence, dans la réalité sociale, de la société de surveillance en tant que phénomène plutôt qu'une abstraction a servi de cause et de moteur au rassemblement, dans le monde universitaire, d'études autrefois éparses et de leurs acquis respectifs pour créer un champ nouveau : les « surveillances studies ».

Au sein de cette sphère particulière, penser en termes de société de surveillance implique de choisir un point de vue, une façon d'aborder le monde contemporain. C'est mettre en évidence non seulement nos rencontres quotidiennes avec la surveillance, mais aussi son caractère de masse qui sous-tend désormais toute l'existence moderne⁶⁶. Dans cette optique, il est nécessaire d'adopter une démarche multidisciplinaire ; tant la sociologie que le droit, en passant par l'informatique, permettent d'ébaucher une opinion pertinente et nuancée sur les facettes de la surveillance. L'adoption d'une telle démarche permet aussi bien au profane qu'à l'expert aguerri d'éviter l'écueil d'une représentation tronquée de la société.

Par ailleurs, et pour souligner l'importance d'une méthodologie rigoureuse dans l'examen de ce phénomène, il est utile de mentionner que la surveillance s'inscrit, de nos jours, dans un important débat qui ne peut être mené que sur de solides bases scientifiques. Celui-ci repose intrinsèquement sur la question de savoir si nous sommes à l'heure actuelle dans une société de surveillance. « Nous vivons indubitablement au sein d'une telle société »⁶⁷. À l'instar d'Éric Delbecque, de nombreuses voix s'élèvent à l'encontre de l'avènement d'une société de surveillance généralisée, vision pessimiste de la société et de ses transformations comparable à la pensée d'Orwell. D'autres auteurs, beaucoup plus mitigés, estiment par contre l'avènement d'un *Big Brother* improbable. Un tel débat se manifeste avec fracas, chacun arguant selon ses convictions certains traits constitutifs de ce phénomène.

⁶⁶ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 1.

⁶⁷ E. DELBECQUE, *Idéologie sécuritaire et société de surveillance : le storytelling du XXI^e siècle*, Paris, Vuibert, 2015, p. 12.

Dans ce cadre, la présentation de ce qu'est une société de surveillance constitue la troisième partie de notre recherche, mue par plusieurs motivations. La première se rapporte à la volonté d'apprécier lors de la quatrième et dernière partie de notre étude son possible établissement au sein de notre zone territoriale de recherche. En effet, pour évaluer l'éventualité d'une chose, il est nécessaire, au préalable, d'en connaître les différents contours. La seconde motivation est sous-tendue par le manque criant d'informations, dans l'opinion publique, concernant les diverses pratiques de surveillance mises en place au sein de la société. Le grand public peut être partagé, indécis sur le sujet. Toutefois très peu de personnes ont, en réalité, conscience des tenants et aboutissants de ces pratiques dont on estime qu'elles relèvent plus de la science-fiction alarmiste que de la vie réelle. Un tel constat explique ainsi la vision biaisée d'une large partie de la population autour de ce phénomène dès lors que l'on souhaite en débattre. Notre contribution vise par conséquent à mieux appréhender la notion générale de la société de surveillance à travers ses principales caractéristiques distinctives et universelles : sa définition et les confusions basiques à éluder, ses mécanismes ainsi que les technologies sur lesquelles elle repose.

2. Un premier regard sur la Société de Surveillance

La société de surveillance est un phénomène protéiforme eu égard à ses nombreuses manifestations au sein de la collectivité. Sa description est de la sorte aussi complexe que vitale pour celui qui souhaite apprécier un concept particulier ; c'est d'autant plus vrai lorsque le terme en question est – comme celui de notre étude – ambigu et controversé. Dans plusieurs essais, la notion de surveillance se limite à la collecte d'informations diligentée exclusivement par les gouvernements et leurs agences. Dans d'autres, elle est à ce point vaste qu'il devient laborieux de cerner les caractéristiques et la réalité censée être décrite. L'objet de ce chapitre consiste ainsi à décrire sommairement la société de surveillance avant d'aborder en profondeur, dans les chapitres suivants, ses mécanismes et les technologies mobilisées en son sein.

Plus précisément, dans les développements subséquents, nous souhaitons offrir au lecteur de ces lignes quelques clés d'analyse succinctes et nécessaires pour apprécier de manière nuancée une telle réalité. Dans la première section de ce chapitre, nous procédons d'abord à la définition de la société de surveillance et de ses principales composantes. Dans la seconde section, nous mettons ensuite en lumière certains éléments propres à porter confusion au sujet de ce phénomène.

2.1. Définitions

La société de surveillance peut être définie comme étant une société dont l'organisation et la structure reposent sur l'utilisation technique de surveillance⁶⁸. Être sous surveillance signifie de la sorte que les renseignements relatifs à nos déplacements et activités personnelles sont enregistrés, essentiellement par des moyens techniques, pour le compte d'organisations privées et des gouvernements qui structurent notre société⁶⁹. En définitive, l'acquisition temporaire, permanente ou à durée variable, par tout procédé de quelque nature que ce soit d'informations constitue l'essence de toute pratique de surveillance au sein de cette société⁷⁰. Pour affiner cette définition générale sur une telle société, il est nécessaire d'en expliciter ses principales composantes : les données, les pratiques et l'objet de la surveillance.

⁶⁸ C. LAVAL, *op. cit.*, p. 69.

⁶⁹ *Ibidem*.

⁷⁰ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 3.

Le concept de la société de surveillance suppose une attention soutenue envers certaines données. Visuelles, auditives, informatiques ou issues du corps analysé, celles-ci sont multiples et innombrables. Elles sont généralement produites par nos actions quotidiennes ou l'usage de certaines technologies numériques, notamment celles de l'information et de la communication, dont l'objectif est de faciliter ces agissements. « La donnée collectée peut porter sur un individu particulier, sur un type d'individu, sur un endroit où des personnes non identifiées au préalable ont été détectées, sur des traces informatisées de transactions diverses sur Internet et dans le monde physique »⁷¹.

La capacité de recueillir une quantité considérable d'informations sur une foule d'objets variés caractérise assurément les pratiques contemporaines de surveillance, qu'elles soient assistées par une base technologique, ou non⁷². Celles-ci constituent une composante essentielle de la société de surveillance puisqu'elles s'érigent en trait d'union entre une donnée brute et son analyse. En effet, ces données sont captées, triées, étudiées et catégorisées par des pratiques en constante sophistication pour servir de base à des décisions qui affectent quotidiennement notre existence⁷³. Notons que de telles décisions concernent directement l'accès au travail et à la sécurité sociale, à l'aide médicale, aux biens et services ou à la justice pénale, voire même à la liberté de mouvement et de déplacement dans la sphère publique pour tout individu dont les activités sont scrutées à des fins judiciaires ou commerciales.

Enfin, l'objet de la surveillance forme un dernier élément de cette société. Il s'agit principalement des personnes et de leurs interactions, qu'elles soient personnellement et spécifiquement surveillées, ou qu'elles se situent dans un champ de surveillance portant sur une population, sur un territoire ou sur un flux d'informations numérisées⁷⁴. La surveillance d'un aménagement urbain, public ou privé, et ses attributs matériels consiste dans ce cadre à identifier et contrôler les comportements proscrits, peu importe qui s'y adonne⁷⁵. En outre, « lorsque qu'on surveille des machines, des processus automatisés ou des transactions financières, c'est généralement parce qu'on peut supposer que des personnes en sont directement ou indirectement responsables ou dépendantes »⁷⁶.

⁷¹ S. LEMAN-LANGLOIS, « Introduction : Qu'est-ce que la surveillance ? », In *Sphères de surveillance*, sous la dir. de Stéphane Leman-Langlois, Montréal, Presses de l'Université de Montréal, 2011, p. 10.

⁷² *Ibid.* p. 11.

⁷³ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 4.

⁷⁴ S. LEMAN-LANGLOIS, *op. cit.*, p. 10.

⁷⁵ *Ibidem.*

⁷⁶ *Ibid.* pp. 10-11.

2.2. « What is wrong with a Surveillance Society? »

La société de surveillance est devenue un sujet prisé par un nombre toujours plus important de chercheurs et d'hommes de lettres. Leurs apports diversifiés sont indéniables. Il est toutefois nécessaire de conserver un regard critique sur ces écrits qui conduisent certaines réflexions intellectuelles vers un raisonnement erroné. Nous avons, dans ce mémoire, délibérément choisi de nous écarter de plusieurs propositions émises par d'éminents auteurs tels que Bentham et Deleuze dont nous estimons qu'elles ne sont pas, ou plus, d'actualité. Ainsi, « cantonner toute réflexion au panoptique de Bentham, cette prison modèle parangon des sociétés disciplinaires, ou la réduire à l'analyse de Deleuze sur le contrôle démocratique permanent en espace ouvert, conduit à une même myopie conceptuelle »⁷⁷.

Dans les développements ci-dessous, nous souhaitons mettre l'accent sur plusieurs éléments essentiels pour apprécier pleinement la réalité de l'objet étudié. Dans un premier temps, nous soulignons deux confusions courantes à propos de la société de surveillance. Dans un second temps, nous ébauchons le caractère ambivalent des effets de la surveillance.

2.2.1. Deux confusions à éluder

Lors de la deuxième partie de notre étude, nous avons abordé une série de différents facteurs dont la réunion serait une indication probable de l'émergence d'une société de surveillance. Le principal message se dessinant en filigrane était le développement conséquent de pratiques de surveillance dans le contexte d'une société en pleine expansion vers une certaine modernité.

Comprendre la société de surveillance comme produit de la modernité nous permet d'éviter de tomber dans un premier piège, celui de la surveillance comme complot ourdi par une autorité totalitaire⁷⁸. La société occidentale avec son modernisme accentué se base sur une assise technologique et morale⁷⁹. La surveillance procède intimement de la même logique : c'est en raison de l'émergence de nouveaux moyens technologiques concomitante à celle d'une perception morale différente de l'insécurité que les pratiques de surveillance ont pu se

⁷⁷ D. FOREST, *Abécédaire de la société de surveillance*, Paris, Syllepse, 2009, pp. 3-4.

⁷⁸ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 2.

⁷⁹ Voy. les différents facteurs explicités ci-dessus.

développer. Elles ne sont, en aucun cas, le fruit en Occident d'une autorité étatique motivée par un dessein néfaste et pernicieux.

Il est illusoire de croire, dans un second temps, que la surveillance est uniquement produite par les nouvelles technologies⁸⁰. Cette affirmation est le deuxième piège que nous souhaitons éviter aux lecteurs de ces lignes. Certes, les pratiques de surveillances se basent énormément sur des supports technologiques. Pourtant, nombre d'entre elles ne font pas appel aux nouvelles technologies comme la simple observation ; l'écoute et la filature tant de la part des services de police que des citoyens lambdas ; le recours fréquent à des espions, des agents d'infiltration et des informateurs de la police et des services de sécurité ou l'utilisation de dossiers écrits. Ainsi, « la surveillance n'a pas été inventée à l'ère des ordinateurs, d'Internet et de la numérisation »⁸¹.

Il existe également de nombreuses situations de « surveillance sociale » où les citoyens ordinaires entrent de plain-pied dans des mécanismes de politique de sécurité et de vigilance⁸². En janvier 2002, le département américain de la justice annonça la création d'un programme intitulé « Terrorism Information and Prevention System ». L'objectif poursuivi par l'administration du président Bush était de recruter des millions de travailleurs américains ayant un accès facilité au logement tels que des plombiers, serruriers, ou techniciens de câble afin de rapporter au gouvernement et à la police toute activité jugée inhabituelle ou suspecte en lien avec le terrorisme⁸³. Si ce programme fut abandonné par les autorités américaines suite au tollé provoqué au sein de l'opinion publique, d'autres projets étroitement liés au TIPS furent très rapidement adoptés. Le Marine Watch programs, le Highway Watch, le « CAT Eyes », le Real Estate Watch ou le Florida's TIPS sont autant d'exemples démontrant un possible « enrôlement » du citoyen au sein d'une « surveillance sociale »⁸⁴.

En Angleterre, des « Neighbourhood Watch » ont vu le jour sous l'impulsion du ministère de l'Intérieur. Ces programmes désignent l'action d'un ensemble de personnes d'un quartier ou d'une rue qui s'associent dans le but de prévenir, par une vigilance active, tout agissement

⁸⁰ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 2.

⁸¹ G. MARQUIS, « Private security and surveillance : from the dossier « society » to database networks », In *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003, p. 226.

⁸² *Voy.* Section 2.5. p. 28.

⁸³ J. STANLEY, *op. cit.*, p. 3.

⁸⁴ *Ibid.*, p. 5.

délictueux. La Belgique, comme nous l'avons brièvement mentionné précédemment, s'est également pourvue de plans d'actions similaires au Neighbourhood Watch britannique. Ainsi, depuis 1998, il est légalement possible de mettre en place un « réseau d'information de quartier » au sein duquel une association structurée de riverains veille sur un territoire délimité⁸⁵. De telles participations citoyennes de surveillance se sont enfin développées en Allemagne, en Australie, en Suisse et dans quelques villes françaises.

Cette surveillance dépourvue de supports technologiques n'échappe guère aux critiques. Tout d'abord, les injonctions de signaler tout acte anormal sur lesquelles se fondent la plupart de ces programmes ne concernent pas, ou très peu, des crimes dont la commission est déjà survenue. Ces derniers se basent insidieusement sur la perspective ou la suspicion que des individus sont susceptibles de planifier quelque chose de malveillant⁸⁶. Nous retrouvons le mirage d'une surveillance non pas axée sur la résolution de crime mais sur leur éventuelle prévention⁸⁷. En outre, l'efficacité de ce genre de mesures est très relative. D'une part, de nombreux comportements visés par les autorités n'ont aucun rapport avec des faits de nature délictueuse ou criminelle. Pourtant il s'agit de l'objectif invoqué par les différentes autorités compétentes pour la mise en place de ces moyens d'action. D'autre part, ces exhortations constantes emportent avec leur application de nombreuses conséquences sociales alarmantes, à l'instar de dénonciations calomnieuses ou racistes dont pourrait être l'objet un individu ou un groupe d'individus stigmatisés comme étant déviants⁸⁸.

Tandis que l'attention se concentre principalement sur les technologies avancées de surveillance, il ne faut pas oublier à quel point les formes primaires de surveillance ont toujours été importantes tout au long de l'histoire⁸⁹. La surveillance n'est ainsi pas inhérente, comme nous pourrions le croire, à des technologies de plus en plus sophistiquées. Ces dernières ne constituent, *in fine*, que le support et la base matérielle par le biais desquels elle s'exerce.

⁸⁵ Pour plus d'information, voir notamment la Circulaire ministérielle du 2 juillet 2001 relative aux réseaux d'information de quartier ; V. SERON & S. SMEETS, *Participation citoyenne et sécurité publique. Enjeux émergents et expériences locales*, Bruxelles, Politea, 2006 ; M. CUSSON, *Prévenir la délinquance. Les méthodes efficaces*, Paris, PUF, 2002 ; P. MARY & Y. CARTUYVELS, « Le plan fédéral de sécurité », *Courrier hebdomadaire du Crisp*, 2001, pp. 5-63.

⁸⁶ J. STANLEY, *op. cit.*, p. 4.

⁸⁷ *Voy.* Section 2.1. p. 19.

⁸⁸ J. STANLEY, *op. cit.*, p. 7.

⁸⁹ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 16.

2.2.2. *L'ambivalence des effets de la surveillance*

La surveillance est un concept à double face dont il convient de souligner le caractère ambivalent de ses répercussions. Un commentaire sur ce trait particulier ambitionne principalement de replacer les pratiques de surveillance dans leur contexte afin de pouvoir identifier avec vigilance les problèmes clés et leurs propositions de solution.

Prenons tout d'abord les effets positifs. En termes de justice ou de liberté, la surveillance accrue n'est pas douteuse en soi⁹⁰. « Que l'on songe à l'utilisation de caméras de vidéosurveillance dans les salles d'interrogatoire de la police, qui encouragent plus qu'elles ne gênent le traitement équitable des suspects »⁹¹. De surcroît, il est aisément compréhensible que la surveillance présente certains bénéfices dans la poursuite et la répression de certains crimes et délits, notamment par sa capacité à cumuler toute une série d'informations et de données sur un individu particulier. Martine Michel, juge d'instruction à Charleroi, confirme ce point de vue lorsqu'elle affirme que la surveillance et les nouvelles technologies utilisées dans ce cadre offrent « *de nombreuses informations développées notamment sur la localisation, sur les contacts que la personne aurait avec X ou Y et puis sur les informations qu'elles donnent via ces moyens technologiques* »⁹². Ainsi, tant des réseaux terroristes que des associations criminelles en matière de stupéfiants par exemple peuvent être démantelés avant la commission d'un crime ou délit par la connaissance dont les services de police disposent sur l'identité, l'organisation et les futures actions des membres du groupe surveillé.

Si la surveillance procure certains effets positifs, elle présente, *a contrario*, concomitamment certains corollaires à risques et inconvénients indéniables. Les chercheurs britanniques de l'association caritative « Surveillance Studies Network » estiment que les infrastructures technologiques et la surveillance de grande ampleur sont prédisposées à engendrer des problèmes d'une ampleur tout aussi importante⁹³. Pouvons-nous accepter de voir notre vie privée, notre liberté d'action et de mouvement s'effacer au profit d'une surveillance, généralisée et intrusive, motivée par des objectifs sécuritaires ? Malheureusement, plusieurs exemples illustrent cette réalité bien réelle. De nombreux américains d'origine musulmane se sont vu ainsi refuser le droit de voyager parce que leur nom est inscrit sur des « No Fly Lists »

⁹⁰ D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », *op. cit.*, p. 93.

⁹¹ *Ibidem*.

⁹² Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

⁹³ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 2.

ou ont fait l'objet d'un profilage discriminatoire au motif unique de leur appartenance religieuse⁹⁴. Dans ce cadre-là, le témoignage du journaliste Herb Boyd est alarmant : « *Au cours d'un vol à destination de Detroit en Décembre 2001, je remarquai que mon billet avait un point rouge. Je n'y ai pas prêté attention jusqu'à ce que je découvre que nous étions plusieurs dans la même situation, tous clairement identifiables comme étant Arabe ou d'origine arabe. Nous étions tous virtuellement dévisagés avant d'entrer dans l'avion* »⁹⁵.

Ces pratiques illustrent parfaitement un risque évident qu'engendre une surveillance accrue. À cet égard, les chercheurs de la Surveillance Studies Network ne tolèrent expressément pas la mise en place de telles mesures extraordinaires et inhabituelles pour la poursuite d'un supposé « bien commun »⁹⁶. La surveillance est, dans un contexte particulier, une menace contemporaine aux libertés individuelles⁹⁷. En outre, ses effets peuvent être encore plus néfastes puisque, comme l'illustre l'exemple ci-dessus, elle est un puissant moyen de créer et de renforcer les discriminations sociales à long terme.

Le caractère ambivalent de la surveillance et de ses effets est, en conclusion, consécutif à la vision biaisée que nous pouvons nous en faire⁹⁸. Pour David Lyon, la surveillance en tant que telle n'est pas lugubre ou pernicieuse. Toutefois, l'attention accrue portée sur un groupe d'individus dans le but de les influencer, de les gérer ou de les contrôler n'est pas innocente non plus⁹⁹. Il est donc important de pouvoir resituer dans le contexte et les circonstances de l'espèce le développement des pratiques de surveillance dans le but de les analyser, de les apprécier et de les commenter. Pour notre part, nous estimons que les divers dispositifs technologiques de surveillance ne sont *à priori* ni positifs, ni négatifs. C'est dans certaines circonstances que l'intensification de mesures de surveillance peut avoir des effets sociaux négatifs : quand la prescription prend le dessus sur la protection, et le contrôle sur le soin¹⁰⁰. La surveillance doit ainsi pouvoir être étudiée dans son environnement particulier à l'instar de ses circonstances qui peuvent exacerber des conséquences sociales néfastes et préjudiciables.

⁹⁴ AMNESTY INTERNATIONAL USA, *Threat and Humiliation : Racial Profiling, Domestic Security and Human Rights in the USA*, New York, Amnesty International USA, 2004, p. 8.

⁹⁵ *Ibidem*.

⁹⁶ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 2.

⁹⁷ D. LYON, *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003, p. 88.

⁹⁸ D. LYON, *The electronic eye : the rise of surveillance society*, Cambridge, Polity Press, 1994, p. 219.

⁹⁹ D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », *op. cit.*, p. 93.

¹⁰⁰ *Ibidem*.

3. Les mécanismes de la Société de Surveillance

Précédemment, nous avons abordé différentes explications possibles que nous estimons être pertinentes pour rendre compte et apprécier les fondations de notre objet d'étude. En termes de surveillance, la société contemporaine repose sur une assise organisationnelle et structurelle étroitement liée aux volontés politico-sécuritaires d'observation d'un grand nombre d'individus. Celle-ci fonctionne ainsi, en partie, sur la base de l'extensification de collectes d'informations personnelles, de l'enregistrement, du stockage, de l'analyse et de l'application de ces données collectées aux individus et groupes concernés.

Les cartes de fidélité, les sites web et leurs cookies, le dépistage commercial des routines et des habitudes d'achat ou la localisation d'un téléphone portable par le biais des antennes-relais sont autant de pratiques axées sur la surveillance au sein de la société que nous étudions dans cette recherche. Chacune poursuit, dans une mesure différente, la réalisation d'un but spécifique : contrôler, réguler, gérer ou influencer un groupe d'individus.

Dans la poursuite de tels objectifs, plusieurs mécanismes-clés constituent à l'heure actuelle le cœur du fonctionnement de la société de surveillance. Ce chapitre est ainsi consacré à l'étude de ces mécanismes. Nous abordons successivement le partage de l'information – le détournement d'usage – ainsi que le tri social, la catégorisation et le ciblage.

3.1. Le partage de l'information

L'essor de l'Internet et des technologies numériques bouleversa profondément l'assise fonctionnelle de la société. Autrefois définie par son industrialisation, la société contemporaine et son écosystème numérique se caractérise désormais par une connexion toujours plus dense des individus. « Ce qui passe pour une nouveauté sans précédent, ce sont, entre autres, les supports technologiques de l'information, ou plus explicitement les nouvelles technologies de l'information et de la communication »¹⁰¹. Cette révolution inédite, non plus industrielle mais numérique, se traduit par une dématérialisation des nouvelles formes de communication et de leur mise en réseau. Désormais, « le réseau des objets connectés » est une réalité tangible ! Par le biais de puces électroniques, des réseaux wifi ou bluetooth, de

¹⁰¹ G. BERTHOUD, *op. cit.*, p. 155.

nombreux biens de consommation sont de plus en plus reliés à l'Internet permettant de concrétiser le concept d'ubiquité de la connectivité des personnes et de leurs données dans le temps comme dans l'espace¹⁰². À l'écoute de nombreux commentateurs, nous serions tous inéluctablement entraînés dans une « mutation informationnelle » dans laquelle la donnée personnelle bénéficierait d'une place fondamentale dans la société actuelle et la gestion de ses individus¹⁰³.

L'introduction majeure, au sein de la société numérique, des technologies de l'information et de la communication a engendré une surmultiplication des informations, codées et stockées sur des supports informatisés. Considérée comme le « pétrole numérique » du XXI^e siècle, la donnée personnelle occupe dorénavant, dans les pratiques de surveillance, une place centrale pour le contrôle et la gestion d'un groupe d'individus. « Plus nous diversifions notre présence numérique, plus nous laissons d'indices, et plus il y a de traces à suivre, plus notre profil se complexifie »¹⁰⁴. Constamment, nous abandonnons une multitude de traces qui informent les autorités étatiques de notre identité, géolocalisent l'ensemble de nos déplacements, dévoilent tant nos choix que nos idées les plus intimes. Du téléphone portable aux cartes à puce en passant par la navigation sur le net, la source de ces données numériques et leur enregistrement sont aussi divers que variés.

La connexion et le partage – entre états, organismes ou services – de toutes ces informations nominales émanant de multiples bases de données pourraient, dans un avenir proche, faire de chacun un être transparent et comme tel aisément contrôlable dans ses activités¹⁰⁵. N'est-ce pas là l'objectif principal de la surveillance contemporaine ? Pour contrôler, influencer et réguler une population donnée, la surveillance doit donc se baser avant toute chose sur un mécanisme de partage des informations personnelles entre divers acteurs rendu possible grâce au nouveau paradigme de la communication explicité ci-dessus. Telle est l'essence de ce mécanisme dont nous souhaitons développer les principales caractéristiques. Plus précisément, nous approfondirons dans les sous-sections suivantes deux dimensions essentielles permettant de rendre compte avec précision de la réalité du mécanisme de partage de l'information dans la société de surveillance. Tout d'abord, une attention particulière sera accordée aux bases de données. En effet, pour qu'une information puisse être partagée, celle-

¹⁰² M. ALBERGANTI, *Sous l'œil des puces : la RFID et la démocratie*, Arles, Actes Sud, 2007, p. 86.

¹⁰³ *Ibidem*.

¹⁰⁴ L. MERZEAU, « Du signe à la trace : l'information sur mesure », *Hermès, La Revue*, 2009, vol. 1, p. 27.

¹⁰⁵ G. BERTHOUD, *op. cit.*, p. 160.

ci doit nécessairement être, au préalable, stockée dans des supports adéquats. La base de données constitue donc un outil informatisé primordial dans la mise en œuvre d'un partage à grande échelle de l'information. Ensuite, nous illustrerons ce mécanisme avec une tendance contemporaine fondamentale : la contribution des entreprises commerciales dans le partage de l'information. C'est dans ce contexte que celui-ci s'éclaire parfaitement.

3.1.1. La base de données

L'établissement de fichiers constitue une dimension indissociable de la relation entre les surveillants et les surveillés. « Chaque individu doit être identifié avec la plus grande précision : nom, date et lieu de naissance, ascendance familiale, description physique, lieu d'habitation, activités... selon des caractéristiques transhistoriques »¹⁰⁶. La volonté constante de contrôler les risques et les menaces de la société tend ainsi à la récolte, à l'archivage et au partage des données.

Les bases de données, au cœur des pratiques de surveillance, ont régulièrement évolué en fonction des différentes techniques d'écriture et de mémorisation¹⁰⁷. Autrefois fixés sur des registres écrits et imprimés, les gigantesques volumes contemporains de stockage informationnel sont désormais le résultat exclusif de traitements électroniques et dynamiques endossant une nouvelle dimension immatérielle et invisible¹⁰⁸. Dès 1988, Gary T. Marx notait ainsi l'importance des archives stockées sur ordinateur qu'il estimait être à la base du fonctionnement d'une « société de dossiers »¹⁰⁹. Conséquemment, l'évolution des technologies informatiques modifia au fur et à mesure les modes de saisie de l'information, d'après une courbe toujours plus ascensionnelle amplifiant le volume des données conservées et le perfectionnement taxinomique des individus¹¹⁰.

Dans le sillage de ces transformations électroniques, une masse toujours plus importante de traces numériques se concentre sous une architecture informatisée sans commune mesure. Le recours aux fonds informationnels numériques, ou bases de données, offre aux différents acteurs une multitude d'informations personnelles sur le comportement d'une personne. Nos

¹⁰⁶ É. SADIN, *op. cit.*, p. 109.

¹⁰⁷ *Ibid.*, p. 110.

¹⁰⁸ *Ibid.*, pp. 110-111.

¹⁰⁹ G. T. MARX, « La société de sécurité maximale », *Déviance et Société*, 1988, vol. 12, p. 152.

¹¹⁰ É. SADIN, *op. cit.*, p. 110.

gestes quotidiens produisent au sein de la société de surveillance des codes dont l'existence immatérielle génère « un dédoublement de la personne sous la forme de calques virtuels et de profils actualisés en permanence »¹¹¹. Toute action est ainsi analysée et traitée à distance des corps physiques au sein de leur équivalent numérique accumulé dans plusieurs bases de données. Motivé par le souhait de contrôler et de gérer des comportements particuliers, la constitution de ces innombrables fonds informationnels sur les citoyens et le partage de leurs contenus sont désormais au cœur du fonctionnement des entreprises privées et des services publics¹¹².

Suite à ces considérations générales, nous souhaitons approfondir plusieurs dimensions particulières d'une base de données. Tout d'abord, nous mentionnons les fondements légaux en droit belge de ces « dossiers numérisés ». Ensuite, nous abordons brièvement leur fonctionnement pour, enfin, illustrer ce mécanisme de partage de l'information par le biais d'une base de données avec un exemple contemporain.

3.1.1.1. La base de données dans la loi belge

En Belgique, le législateur s'est rapidement pourvu d'un texte légal spécifique en matière de collecte des données à caractère personnel. Dans cette optique, il adopta la loi du 8 décembre 1992, couramment appelée « loi vie privée », visant à garantir au citoyen le respect de son droit à la vie privée lors de la manipulation par différents acteurs de ces données¹¹³. Ce prescrit légal fournit quelques indications sur les bases de données.

Tout d'abord, la loi du 8 décembre 1992 définit la notion de base de données. « Pour l'application de la présente loi, on entend par fichier, un ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »¹¹⁴. À noter que le Code de droit économique définit également une telle notion. Celle-ci n'est toutefois limitée qu'au domaine commercial. « Les définitions suivantes sont applicables au livre XI. (...) La base de données est un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de

¹¹¹ É. SADIN, *op. cit.*, p. 115.

¹¹² SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 20.

¹¹³ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

¹¹⁴ Art. 1, § 3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière »¹¹⁵.

Après avoir défini l'objet de cette sous-section, la « loi vie privée » oblige tout gestionnaire d'une base de données à déclarer, auprès de la commission de la vie privée, la constitution de ce fond informationnel¹¹⁶. « Préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées, le responsable du traitement en fait la déclaration auprès de la Commission de la protection de la vie privée. La déclaration doit mentionner (...) la finalité ou l'ensemble des finalités liées du traitement automatisé »¹¹⁷. Jean-François Joris, Commissaire au Regional Computer Crime Unite de la Police Judiciaire Fédérale de Liège, explicite cette obligation :

*« Toute banque de données en Belgique doit être déclarée auprès de la commission de la vie privée, sinon elle est illégale. Chaque champ qui la compose et sa structure (nom, prénom, sexe, adresse, achats principaux,...) doit être spécifié et les finalités, judiciaires, commerciales ou autres, de la constitution de la banque de données doivent être précisées dans la déclaration »*¹¹⁸.

Il en résulte que le responsable d'un fond informationnel ne peut collecter des données personnelles incompatibles avec la poursuite de la finalité initialement mentionnée dans la déclaration. Ainsi, un commerçant ne peut dans le cadre de ses activités économiques recueillir des informations relatives à la date de naissance et à la profession de ses clients. Une obligation de transparence est en conséquence imposée au gestionnaire, tant au niveau de l'existence de la base de données que de la récolte de ces dernières.

Enfin, le législateur belge envisage clairement la possibilité d'un partage interétatique de l'information ! Deux situations doivent nécessairement être distinguées, selon que le pays destinataire d'un tel partage est, ou non, membre de l'Union européenne.

¹¹⁵ Art. I.13., 6° du Code de droit économique.

¹¹⁶ La Commission de la protection de la vie privée est un organisme indépendant créé par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Elle veille à ce que les données à caractère personnel soient traitées dans le respect de ladite loi, de manière à préserver la vie privée des citoyens.

¹¹⁷ Art. 17, § 1 & 3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

¹¹⁸ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

D'une part, les données à caractère personnel peuvent circuler librement depuis la Belgique au sein des pays de l'Union européenne, pour autant que les principes généraux relatifs à la protection des données de la loi belge soient respectés. Suite à l'adoption de la Directive européenne 95/46/CE relative à la protection du traitement des données à caractère personnel et à la libre circulation de ces données, les États membres appliquent un même niveau de protection¹¹⁹. Un transfert au sein de l'Union européenne est par conséquent librement autorisé. Notons qu'une multitude de situations quotidiennes est ainsi régie par cette directive. Par exemple, une agence de voyage belge peut envoyer à la compagnie aérienne française et à l'hôtel espagnol réservé par son client les données de celui-ci, une banque peut envoyer les informations relatives à un de ses clients pour effectuer un paiement en France, etc¹²⁰.

L'article 21 de la loi du 8 décembre 1992 permet, d'autre part, le transfert sous condition de données de la Belgique vers un pays hors de l'Union européenne. « Le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution. Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données (...) »¹²¹. La Commission européenne a notamment admis le caractère adéquat du niveau de protection des pays suivants : la Suisse, le Canada, Andorre, l'Argentine, les États-Unis, le Guernesey, les îles Féroé, l'île de Jersey et l'île de Man, l'Australie, l'Islande, le Liechtenstein et Israël. Toute autorité ou entreprise souhaitant importer des données à caractère personnel hors de l'Union européenne doit ainsi se renseigner sur le niveau de protection adéquat du pays destinataire et le respecter. Notons que si le pays ne présente pas un niveau adéquat de protection, le responsable du traitement peut offrir lui-même, par la voie contractuelle, une protection appropriée¹²².

¹¹⁹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>, consulté le 2 avril 2016.

¹²⁰ Pour plus d'exemples, voir notamment :

<https://www.privacycommission.be/sites/privacycommission/files/documents/protection-donnees-a-caractere-personnel-en-belgique.pdf>, consulté le 28 mars 2016.

¹²¹ Art. 21, § 1 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

¹²² Art. 22, § 1 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel : « Le Roi peut autoriser un transfert de données à caractère personnel vers un pays non membre de la Communauté européenne n'assurant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et droits fondamentaux des personnes ; ces garanties peuvent notamment résulter de clauses contractuelles ».

En définitive, le législateur belge s'est adapté aux transformations sociétales eu égard aux évolutions technologiques. Le droit reconnaît de la sorte la situation dans laquelle le responsable d'une base de données peut s'adresser directement à diverses institutions ou entreprises pour obtenir certaines informations personnelles sur une personne déterminée. Le partage de l'information est ainsi pleinement reconnu au sein de la société.

3.1.1.2. Le fonctionnement d'une base de données

Actuellement, toute base de données est intimement liée au développement des technologies numériques et de leurs processus computationnels. De tels mécanismes permettent de réduire l'élément étudié en une séquence de chiffres « produisant une mise à plat haute définition et systématisée d'ensembles informationnels initialement plus compacts »¹²³. Pour ce faire, nous retrouvons au sein de chaque fonds informationnel numérique un « système de gestion de base de données » consistant à stocker et à partager des informations dans une telle base, en garantissant la qualité, la pérennité et la confidentialité des informations. Ce logiciel, composé d'une suite de programmes, manipule la structure de la base de données et gère l'accès aux données qui y sont stockées.

Au sein de ce système de gestion, le bit, à savoir l'unité de mesure en informatique, permet lorsqu'il est relié à d'autres « particules » ou bits de produire des fichiers dont la cohérence et la précision sont rendues possibles par un traitement quantifié en un million ou milliard d'unités¹²⁴. Les différentes informations élémentaires du monde physique sont, dans cette optique, divisées selon une procédure de décomposition en une infinité de fragments standardisés pour ensuite subir une recomposition numérique suivant des algorithmes déterminés. Par ces processus informatiques complexes, la base de données se voit ainsi pourvue de la capacité de recueillir et d'analyser un ensemble brut d'informations, de les interpréter et de les partager au sein d'un réseau interconnecté. En somme, le numérique transforme toute réalité factuelle en données informatisées instaurant dès lors un rapport médiatisé aux êtres et aux choses¹²⁵.

¹²³ É. SADIN, *op. cit.*, p. 111.

¹²⁴ Le bit est l'unité la plus simple dans un système de numération, ne pouvant prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1. Un bit ou élément binaire peut représenter aussi bien une alternative logique, exprimée par faux et vrai, qu'un chiffre du système binaire ; É. SADIN, *op. cit.*, p. 111.

¹²⁵ *Ibidem*.

3.1.1.3. Un cas illustratif : le Passenger Name Record

« *Il est plus que jamais nécessaire que l'Europe adopte le texte sur le PNR afin de garantir la traçabilité des déplacements (...). C'est une condition de notre sécurité collective* »¹²⁶. Devant l'Assemblée nationale française, Manuel Valls a souligné, au lendemain des attentats terroristes du 13 novembre 2015, l'importance que revêt à ses yeux le « Passenger Name Record ». Après plusieurs années, ce projet ayant longtemps fait l'objet d'âpres débats a finalement été adopté, le 14 avril 2016 au Parlement européen par 461 voix pour et 179 contre, suite à la pression accentuée par le choc des attentats de Paris et de Bruxelles.

Plus précisément, le Passenger Name Record est une vaste base de données adoptée dans un texte législatif pour prévenir et détecter préventivement les infractions terroristes et les infractions graves¹²⁷. Outre le terrorisme, de nombreuses formes de criminalité, intégrées sous la catégorie « infractions graves », sont visées par ce texte ; du trafic d'armes à la corruption, de l'espionnage industriel au viol, en passant par les crimes environnementaux, la portée de cette directive est extrêmement large. Une collecte, une conservation et un partage plus systématique des « données PNR » permettraient d'intensifier les enquêtes tant proactives que répressives et les poursuites en la matière, motivées selon le Parlement européen par la nécessité de contrer les menaces pesant sur la sécurité¹²⁸.

Ces données PNR sont toutes les informations personnelles communiquées par les passagers de vols aériens et collectées ensuite par les compagnies de transport lors de la réservation d'un vol ou de l'enregistrement¹²⁹. Cette base de données comprend ainsi l'identité de tous les passagers des avions circulant, entrant ou sortant de l'espace européen. Outre l'identité du voyageur, la directive européenne prévoit que les compagnies aériennes doivent collecter une vingtaine de données sur les passagers de vols extra- et intra-européens¹³⁰. Elles concernent les dates du voyage, l'itinéraire, le numéro de téléphone du passager, son adresse courriel, la manière dont il a payé son billet, le numéro de celui-ci, le numéro du siège, ses bagages et son

¹²⁶ <http://www.gouvernement.fr/partage/5883-prorogation-de-l-etat-d-urgence-discours-de-manuel-valls-devant-l-assemblee-nationale>, consulté le 8 mars 2016.

¹²⁷ <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52011PC0032>, consulté le 11 avril 2016.

¹²⁸ <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52011PC0032>, consulté le 11 avril 2016.

¹²⁹ C. VALLET, « Fichés jusqu'au ciel ? », *Alternatives Internationales*, 2015, vol. 3, p. 69.

¹³⁰ J.-P. STROOBANTS, « Accord sur le PNR, le fichier qui regroupera les données des passagers aériens en Europe », *Le Monde*, mis en ligne le 10 décembre 2015, consulté le 7 février 2016. Disponible sur : http://www.lemonde.fr/europe/article/2015/12/10/accord-crucial-sur-le-fichier-europeen-des-passagers-aeriens_4829041_3214.html

éventuel programme de fidélité ou de « voyageur fréquent »¹³¹. Parfois, le nom des hôtels ou le type d'alimentation – choix d'un repas halal ou casher – d'un passager est mentionné. Nous trouvons même, au sein de cette base de données, un espace plus libre où des remarques générales peuvent être faites au sujet du client¹³².

L'ensemble de ces données intégrées au Passenger Name Record est conservé pendant 6 mois alors que le texte initial de la Commission des libertés civiles proposait 30 jours. « À l'expiration de ce délai, (...) tous les éléments d'information pouvant servir à identifier le passager auquel se rapportent les données PNR sont masqués »¹³³. Les informations anonymisées ne sont ainsi accessibles qu'à un nombre restreint d'organisations sous le contrôle d'une autorité judiciaire nationale, en fonction de certaines conditions. Les États membres veillent enfin à ce que celles-ci soient ensuite effacées après 5 années.

Parmi les organismes ayant accès à ces nombreuses informations, la directive européenne prévoit que les services de renseignement européens puissent accéder à ce vaste fichier. Elle envisage également le partage de données des passagers aériens vers certains pays situés en dehors de l'espace européen. A cet effet, le Parlement européen avait notamment approuvé, le 19 avril 2012, un projet d'accord sur le transfert des données PNR de l'Union européenne vers les États-Unis. Selon la motivation de cette entente, « le partage d'informations, et en particulier le transfert de données des dossiers passagers par les transporteurs aériens assurant des vols entre l'Union européenne et les États-Unis, est un moyen utile de combattre la menace qui pèse sur la paix et la sécurité internationale »¹³⁴. Les États-Unis et globalement tout pays disposant d'une protection équivalente à celle accordée en Europe aux données peuvent désormais les recueillir et les scruter sans que les personnes concernées en aient conscience. Par conséquent, pour prévenir et réprimer le terrorisme et les crimes transnationaux, un partage toujours plus important d'informations personnelles a été aménagé entraînant une surveillance exponentielle de nos déplacements.

Liberticide pour les uns, indispensable dans la lutte contre le terrorisme pour les autres, cette directive ouvre la voie au traçage généralisé des passagers européens. Cet exemple dont nous avons ébauché les traits à titre illustratif reflète parfaitement l'importance accrue, dans le

¹³¹ <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52011PC0032>, consulté le 11 avril 2016.

¹³² C. VALLET, *op. cit.*, p. 72.

¹³³ <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52011PC0032>, consulté le 11 avril 2016.

¹³⁴ <http://www.europarl.europa.eu/sides/getDoc>, consulté le 14 avril 2016.

cadre des pratiques de surveillance, du partage de l'information rendu possible grâce aux bases de données. À ce titre, « les bases de données, grâce à leur interconnexion toujours plus aisée techniquement et toujours plus recherchée économiquement et politiquement, apparaissent comme des composantes essentielles d'une régulation technique de la société »¹³⁵.

3.1.2. La contribution des entreprises commerciales

Mues par un désir de *tout voir pour tout contrôler*, les autorités étatiques réalisent de constants efforts pour étendre leur capacité de surveillance. Toutefois, un obstacle se dresse contre cet accroissement sans cesse recherché ; obstacle intimement lié aux limites pratiques de leurs ressources matérielles, du personnel et de l'organisation nécessaire pour surveiller l'ensemble des faits et gestes de la population¹³⁶. En effet, tout service de renseignement ou de police aussi puissant soit-il est limité financièrement. « *À un moment donné, la logique économique prime sur la logique sécuritaire* »¹³⁷. C'est un obstacle crucial que la sécurité américaine et par extension tout service impliqué dans l'exercice de la surveillance cherche à surmonter. Pour ce faire, la plupart des états procèdent de plus en plus à l'enrôlement, volontaire ou forcé, d'acteurs du secteur privé dans leur réseau de surveillance. Le recrutement d'entreprises commerciales par les autorités étatiques permet ainsi de surmonter partiellement cet écueil financier. En conséquence, il existe un véritable lien entre les entreprises commerciales et les agences de sécurité et services judiciaires des pays occidentaux dont nous estimons opportun d'intégrer brièvement dans notre étude.

Cette « privatisation de la surveillance » offre un avantage considérable dans cette quête d'extensification de la surveillance. Outre le contournement de l'écueil explicité ci-dessus, elle permet un échange sans précédent d'informations des entreprises commerciales vers les agences de sécurité élargissant, de ce fait, la portée de leur surveillance ! Ces sociétés privées, regroupant principalement Google – Apple – Facebook – Amazon – et Microsoft, collectent une quantité considérable de données personnelles issues de nos activités quotidiennes. Ces informations peuvent ensuite être partagées par cette privatisation vers différentes agences gouvernementales. Ainsi, l'État, d'un point de vue global, peut bénéficier, par un partage de

¹³⁵ G. BERTHOUD, *op. cit.*, p. 160.

¹³⁶ J. STANLEY, *op. cit.*, p. 1.

¹³⁷ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

l'information, de données qu'il n'aurait pu collecter lui-même. À côté des agences traditionnelles de sécurité, les entreprises commerciales sont désormais amenées à jouer un rôle fondamental dans les pratiques actuelles de surveillance.

La contribution des entreprises commerciales modulant en grande partie le mécanisme de partage de l'information revêt différentes formes. Une telle contribution peut se baser sur le transfert volontaire de données – l'achat d'informations – ou l'usage de mécanismes juridiques. Nous abordons ces différents points ci-dessous.

3.1.2.1. Le transfert volontaire de données

Pour obtenir des informations sur les activités de certains individus, les autorités étatiques n'ont souvent besoin que d'en demander le partage. C'est la première option possible. « De nombreuses sociétés sont prêtes à remettre les détails des achats ou activités de leurs clients sur base d'une simple requête d'une agence de renseignement »¹³⁸. Aux États-Unis, de nombreuses entreprises estiment ainsi que ce partage relève simplement d'une exigence patriotique. « Quand celles-ci prêtent attention aux multiples demandes de l'exécutif et transmettent des informations privées, elles exécutent tout simplement leur devoir patriotique »¹³⁹.

Dans ce libre échange de données, le domaine aérien est un premier exemple. Des compagnies aériennes ont avoué avoir remis à différentes autorités étatiques les dossiers de voyage de leurs clients. Dans chaque cas, l'information partagée était transmise, non pas dans le but de résoudre un crime particulier, mais dans le but d'examiner chaque dossier dans l'espoir d'identifier des terroristes au comportement suspicieux¹⁴⁰. Nous retrouvons encore l'idée d'une surveillance préventive basée sur un risque généralisé. Ainsi, plusieurs sociétés privées dont la compagnie JetBlue ont transmis à un organe du Pentagone plus de cinq millions de dossiers sur ses voyageurs qui furent, ensuite, combinés avec des informations personnelles achetées auprès de Acxiom, un « data aggregator »¹⁴¹. Quand l'affaire de la JetBlue parut dans les journaux, la compagnie Northwest avoua également avoir transmis des

¹³⁸ J. STANLEY, *op. cit.*, p. 10.

¹³⁹ CONGRESSIONAL RECORD, *Proceedings and debates of the 110th congress: first session*, Vol. 153, Pt. 26, 17 December 2007, p. 34545.

¹⁴⁰ J. STANLEY, *op. cit.*, p. 10.

¹⁴¹ R. SINGEL, « JetBlue shared passenger data », *Wired*, mis en ligne le 18 septembre 2003, consulté le 16 mai 2016. Disponible sur : <http://www.wired.com/2003/09/jetblue-shared-passenger-data/>.

millions de données de vols à la NSA¹⁴². En somme, la plupart des grandes compagnies aériennes américaines assurant des vols domestiques et transnationaux desservant notamment la Belgique ont déjà eu recours à ce genre de pratique¹⁴³.

Outre ce domaine particulier, il existe de nombreux autres secteurs au sein desquels des acteurs privés transmettent volontairement certaines informations. Le Boston Globe révèle notamment que 195 universités américaines ont librement fourni des données sur leurs étudiants étrangers au FBI et au Service d'Immigration et de Naturalisation, peu de temps après les attentats du 11 septembre 2001¹⁴⁴. Des organisations professionnelles, des compagnies de voyage et des associations sans but lucratif sont également impliquées dans ce vaste partage volontaire de l'information, démontrant ainsi l'importance de cette tendance à l'heure actuelle¹⁴⁵.

3.1.2.2. L'achat d'informations

Une seconde option ouverte aux autorités et agences gouvernementales dans l'acquisition d'informations personnelles est leur achat auprès de « Data Aggregator »¹⁴⁶. Spécialisé dans la constitution de dossiers numérisés, un agrégateur de données est une organisation qui recueille, compile et analyse des données individuelles provenant tant des cours et tribunaux que des registres commerciaux dans une démarche résolument lucrative d'échange¹⁴⁷. Selon Acxiom, l'un des principaux leaders dans ce domaine, l'objectif de ses équipes « est de donner du sens aux informations clients et de transformer les données clients en opportunités business. Acxiom est capable de traiter même les bases de données les plus volumineuses qualifiées de big data. En dressant la cartographie du cycle de vie du client et en établissant la valeur de ce cycle, nous pouvons identifier les meilleurs clients et faire des analyses prédictives »¹⁴⁸.

¹⁴² ELECTRONIC PRIVACY INFORMATION CENTER, « Northwest Airlines Gave NASA Personal Info on Millions of Passengers; Disclosure Violated Privacy Policy », *Press release*, mis en ligne le 18 janvier 2004, consulté le 16 mai 2016. Disponible sur : <https://epic.org/privacy/airtravel/nasa/pr1.18.04.html>.

¹⁴³ J. STANLEY, *op. cit.*, p. 10.

¹⁴⁴ P. HEALY, « colleges giving proper data on foreign students' finances », *The Boston Globe*, mis en ligne le 3 octobre 2001, consulté le 16 mai 2016. Disponible sur : <https://www.highbeam.com/doc/1P2-8673165.html>.

¹⁴⁵ J. STANLEY, *op. cit.*, p. 11.

¹⁴⁶ Acxiom, Choicepoint, Lexisnexis et Seisint Inc. sont d'importants agrégateurs de données, par exemple.

¹⁴⁷ J. STANLEY, *op. cit.*, p. 12.

¹⁴⁸ <http://www.acxiom.fr/big-data-et-datamining/>, consulté le 23 avril 2016.

De telles informations intelligibles se sont rapidement développées ces dernières années suite à la constitution de ce secteur particulier d'activité. À l'heure actuelle, il existe un véritable marché lucratif d'acquisition et de partage d'informations personnelles. Dans les faits, le gouvernement américain a déjà eu recours à l'achat de ces informations. Choicepoint, un agrégateur de données, a par exemple reconnu avoir conclu un contrat lucratif à hauteur de 8 millions de dollars avec le département de la justice ainsi qu'avec au moins 35 agences gouvernementales¹⁴⁹. Un autre agrégateur de données, Seisint Inc., a notamment reçu plus de 9,2 millions de dollars en subventions du ministère de la Justice et du ministère de la Sécurité intérieure pour l'acquisition de certaines données¹⁵⁰. En résumé, l'information peut dès lors être achetée si elle n'a pas été volontairement partagée.

3.1.2.3. L'usage de mécanismes juridiques

Si une entreprise commerciale ne souhaite pas donner ou vendre ses informations, les autorités étatiques disposent de puissants mécanismes légaux avec lesquels elles peuvent forcer l'entreprise à partager les données personnelles d'individus en sa possession¹⁵¹. Dans le cadre d'une enquête judiciaire ou d'une activité de renseignement, ces autorités peuvent ainsi se baser sur certaines législations particulières pour faciliter la collecte de nos traces et transactions commerciales. Plus précisément, pour assurer un partage pleinement opérationnel de l'information, deux mécanismes sont internationalement prévus par le droit : la rétention de données et l'acquisition de celles-ci selon les besoins des différentes autorités.

Tout d'abord, la rétention des données est consacrée juridiquement dans toute loi, sans distinction de l'autorité étatique qui la promeut, pour s'assurer que certaines informations soient disponibles au sein d'une entreprise lorsque les services de renseignement et de police ont besoin d'en prendre connaissance¹⁵². Les différents législateurs définissent les règles et procédures de conservation des données personnelles que doivent respecter les opérateurs de télécommunication, les fournisseurs d'accès et les hébergeurs de sites web et de courriels¹⁵³. Une telle obligation est ainsi exigée par les États en vue de pouvoir tracer et identifier

¹⁴⁹ J. STANLEY, *op. cit.*, p. 26.

¹⁵⁰ *Ibidem*.

¹⁵¹ *Ibid.*, p. 12.

¹⁵² *Ibid.*, p. 15.

¹⁵³ Art. 3 & 5 de la directive du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication. Notons que cette directive fut annulée par la Cour de justice de l'Union européenne le 8 avril 2014 sans avoir été remplacée. L'Europe demeure à l'heure actuelle dans le flou juridique.

notamment la source d'une communication et sa destination. Ce mécanisme permet, en conséquence, de conserver et de trier l'information par les entreprises commerciales à partir desquelles il est relativement aisé d'en obtenir l'accès et d'en assurer le partage.

Notons à titre illustratif que la Belgique impose la rétention des données à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques. Le premier paragraphe de cet article énonce notamment que « les données de trafic, les données de localisation, les données d'identification d'utilisateurs finaux, les données d'identification du service de communication électronique utilisé et les données d'identification de l'équipement terminal » doivent être conservées. Le troisième paragraphe de cet article 126 explicite cette obligation de rétention en précisant notamment que ces données sont conservées douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Un second mécanisme juridique consiste, ensuite, à conférer aux services de police et de renseignement d'un état des instruments légaux permettant l'acquisition de données personnelles. « Puisque les sociétés privées accumulent de plus en plus de détails à propos de nos transactions, les pouvoirs du gouvernement pour obtenir ces données sont en constant développement »¹⁵⁴. Si les données sont détenues au sein d'entreprises commerciales, encore faut-il pouvoir disposer des moyens pour en assurer le partage. La plupart des pays occidentaux se dotent ainsi de normes spécifiques dans le but de faciliter l'accès et le partage de données. Nous abordons brièvement ci-dessous trois exemples non-exhaustifs pour illustrer ces normes visant à acquérir des données initialement détenues par des entreprises commerciales. Notons que l'accent est mis sur les mécanismes juridiques et non le domaine commercial dans lequel elles interviennent.

Aux États-Unis, le Patriot Act facilite pour les services de renseignement l'accès aux données personnelles des entreprises tout en réduisant le niveau de preuve exigé lors de l'acquisition de celles-ci. La section 215 de cet acte confère ainsi au FBI des moyens légaux pour accéder aux dossiers des clients détenus par les fournisseurs d'Internet et de toutes autres communications en imposant cumulativement une obligation de confidentialité¹⁵⁵.

¹⁵⁴ J. STANLEY, *op. cit.*, p. 12.

¹⁵⁵ B. STEINHARDT & J. STANLEY, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, Washington DC, ACLU, 2003, p. 9.

En Europe, la Commission européenne instaura au début des années 2000 un cadre juridique, dénommé « Safe Harbor », permettant à plus de 4 000 entreprises américaines, basées dans l'Espace économique européen, de transférer vers les États-Unis les données personnelles de leurs clients¹⁵⁶. Grâce à cet accord, le transfert de ces données vers les sociétés mères aux États-Unis ainsi que leur partage et leur analyse au sein de certaines agences de sécurité nationales furent actées. Les services de renseignement disposent dès lors d'un moyen légal pour acquérir certaines informations commerciales et mettre en place une surveillance axée sur celles-ci. Notons que cet accord fut annulé par la Cour de justice de l'Union européenne et remplacé par le « Privacy Shield ». Si le nouvel accord confère un niveau de protection plus important aux données transférées, le principe général de la disponibilité de l'information et de leur partage demeure identique.

La Belgique est également pourvue de mécanismes légaux facilitant l'accès et le partage de données. Parmi ces mécanismes, l'article 126 de la loi du 13 juin 2005, explicité ci-dessus, instaure par exemple une obligation de collaboration dans le chef des entreprises de télécommunication avec certains services. « En vue de la recherche et de la poursuite des visées aux articles 46bis et 88bis du Code d'instruction criminelle »¹⁵⁷, le législateur belge impose, dans ce cadre, aux opérateurs téléphoniques d'assurer la disponibilité de leurs données commerciales en faveur des services de police et de renseignement. Il s'agit d'une obligation fondamentale dont la soumission au préalable à celle-ci conditionne l'octroi d'une licence nécessaire pour la constitution d'une entreprise de téléphonie. Jean-François Vergieu, Senior Risk Operations Manager chez Base, confirme lors de l'entretien que *« pour pouvoir exercer une activité d'opérateur de télécommunication, il est nécessaire, en vue d'obtenir une licence adéquate, de se soumettre à certaines obligations dont celle de collaborer avec les services de police et de renseignement »*¹⁵⁸.

En définitive, si les services de renseignement et la police collectent certaines informations dans le cadre de leurs activités routinières, ceux-ci convoitent tout aussi avidement les données amassées par les autres institutions reconnaissant de la sorte l'importance inhérente de ces informations collectées et stockées dans des bases de données par des banques,

¹⁵⁶ Y. EUDES, « Pourquoi l'accord Safe Harbor sur les données personnelles cristallise les tensions ? », *Le Monde*, mis en ligne le 25 septembre 2015, consulté le 23 mars 2016. Disponible sur : http://www.lemonde.fr/pixels/article/2015/09/25/pourquoi-l-accord-safe-harbor-sur-les-donnees-personnelles-cristallise-les-tensions_4771879_4408996.html.

¹⁵⁷ Art. 126, §2 de la loi du 13 juin 2005 relative aux communications électroniques.

¹⁵⁸ Entretien avec Monsieur Jean-François Vergieu réalisé le 10 février 2016.

bibliothèques, magasins et agences de télécommunications¹⁵⁹. Pour les obtenir, ces différentes autorités gouvernementales recourent, comme nous venons de l'expliquer, au partage volontaire – à l'achat – ou à différents procédés légaux. Un tel mécanisme de partage de l'information – émergeant dans un contexte commercial pour ensuite être transféré vers un secteur sécuritaire ou judiciaire – caractérise par conséquent la société de surveillance actuelle.

3.2. Le détournement d'usage

Une information collectée dans un contexte particulier en vue de répondre à des objectifs primaires est couramment susceptible d'être partagée, comme nous venons de le voir, entre des acteurs privés et publics. Ce mécanisme repose toujours sur une motivation précise ; celle de poursuivre et de rencontrer des objectifs secondaires. Une autorité étatique peut ainsi avoir intérêt à percevoir toute une série de données commerciales pour atteindre ses desseins sécuritaires dans la gestion et le contrôle d'un groupe particulier. Nous pouvons clairement constater que certaines données personnelles, collectées et utilisées pour un objectif et pour remplir une fonction, migrent vers d'autres objectifs et fonctions intensifiant la surveillance et les invasions à l'encontre de la vie privée¹⁶⁰. Ce constat nous amène dès lors à expliciter un second mécanisme de la société de surveillance dépassant toutefois le cadre du partage de l'information, à savoir le détournement d'usage dans les pratiques de surveillance.

Le détournement d'usage est un mécanisme insidieux par lequel des mesures générales de surveillance introduites pour un objectif initialement défini peuvent rapidement développer de nouveaux usages entraînant une expansion de l'attention sur de nouveaux lieux et populations¹⁶¹. Ce mécanisme implique de pouvoir s'appuyer plus particulièrement sur une pratique de surveillance, sur un dispositif technologique ou sur des données existantes pour en détourner l'usage dans le but d'accroître la portée de la surveillance. Un pareil processus est d'autant plus pernicieux qu'il vise, dans cet accroissement considérable de la surveillance, à contrôler, gérer et réguler un nombre toujours plus important d'individus. De ce fait, le détournement d'usage permet la poursuite des mêmes objectifs inhérents au premier mécanisme explicité ci-dessus.

¹⁵⁹ K. D. HAGGERTY, « surveillance, crime and the police », In *The routledge handbook of surveillance studies*, éd. par Kirstie Ball, Kevin D. Haggerty & David Lyon, Abingdon, Routledge, 2012, p. 239.

¹⁶⁰ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 9.

¹⁶¹ K. D. HAGGERTY, *op. cit.*, p. 236.

Afin d'illustrer ce procédé, nous souhaitons nous baser sur l'enquête menée par l'écrivain James Bridle sur la « Congestion Charge Zone » à Londres. Cette zone désigne un périmètre géographique recouvrant le centre-ville de la capitale anglaise soumis à une taxe quotidienne de circulation. Un système sophistiqué de vidéosurveillance a été mis en place pour enregistrer les véhicules entrant et sortant de la zone de péage¹⁶². Pour ce faire, les caméras enregistrent les plaques minéralogiques et prennent plusieurs photos du véhicule pour en identifier l'utilisateur. Utilisant une base de données centrale des véhicules et de leur propriétaire, le système vérifie ensuite, le jour suivant, que pour chaque numéro relevé le propriétaire du véhicule concerné a effectué un paiement. James Bridle donne, dans l'extrait ci-dessous, à propos de la « Congestion Charge Zone » ce qui est l'une des meilleures descriptions de la façon dont le détournement d'usage a lieu :

« Lorsque la zone a été initialement mise en place, le grand public fut informé que ses données seraient uniquement détenues, et régulièrement supprimées, par l'organisme public 'Transport for London' dont la mission est de superviser la circulation dans la ville de Londres. Cependant, en moins de cinq ans, le ministre de l'Intérieur octroya l'accès pour la police métropolitaine à ce système, ce qui leur a permis d'obtenir des copies complètes des données produites par le système.

Cette autorisation d'accéder aux données a été accordée à la police à la seule condition qu'ils ne l'utilisent que lorsque la sécurité nationale est menacée. Mais depuis que les données sont désormais en leur possession, la police les a reclassées comme 'données criminelles' et les utilise désormais pour les questions générales de police, malgré le libellé de l'autorisation initiale. Comme ces informations ne sont pas considérées comme des 'données personnelles' dans la définition de la loi, la police n'est pas tenue de les détruire, et peut conserver les dossiers concernant tous les mouvements de véhicules dans la ville aussi longtemps qu'elle le désire »¹⁶³.

¹⁶² S. DREYFUS, « Un péage en plein cœur de Londres », *Le Monde*, mis en ligne le 17 février 2003, consulté le 18 mai 2016. Disponible sur : http://www.lemonde.fr/archives/article/2003/02/17/un-peage-en-plein-c-339-ur-de-londres_309533_1819218.html?xtmc=congestion_charge_zone&xtr=13.

¹⁶³ J. BRIDLE, « All cameras are police cameras », *The Nor*, mis en ligne le 7 novembre 2014, consulté le 18 mai 2016. Disponible sur : <http://shorttermmemoryloss.com/nor/2014/11/07/all-cameras-are-police-cameras/>.

Dans de nombreux contextes, les caméras de vidéosurveillance représentent ainsi une illustration évidente de détournement d'usage¹⁶⁴. Comme évoqué précédemment, ce mécanisme se base originellement sur des pratiques de surveillance, sur un dispositif technologique ou sur des données existantes. Une multitude de circonstances factuelles est dès lors envisageable. Il n'est cependant pas réalisable, dans le cadre de notre étude, de dresser un portrait exhaustif de l'ensemble de ces situations illustrant ce phénomène¹⁶⁵. Nous pouvons toutefois mentionner, pour enrichir notre propos, que la géolocalisation des individus et des biens par le biais de dispositifs technologiques satellitaires offre également une forte probabilité d'être destinée à d'autres finalités¹⁶⁶. La quantité d'informations sur les activités humaines offertes par ces technologies et leur qualité rendent en effet possible leurs acquisitions à des fins sécuritaires et de surveillance.

Toute mesure générale de surveillance est, en définitive, susceptible d'être insidieusement détournée. Quelles sont les causes d'une telle dérive ? Tout d'abord, la police et les services de renseignement jouent un rôle considérable en reconfigurant des pratiques de surveillance utilisées dans un domaine particulier en fonction de leurs objectifs répressifs¹⁶⁷. Ensuite, ce mécanisme est rendu possible dans la société actuelle « en raison, d'une part, des nouvelles technologies permettant un développement important de données accumulables et, d'autre part, de l'efficacité organisationnelle souvent considérée comme une priorité absolue occultant toute conséquence néfaste de ce détournement »¹⁶⁸.

3.3. Le tri social, la catégorisation et le ciblage

L'un des développements majeurs les plus importants à l'heure actuelle est la façon dont la surveillance, qui était autrefois réservée aux « suspects » ou aux « déviants », est volontairement étendue pour couvrir la majorité de la population¹⁶⁹. Cette expansion est

¹⁶⁴ K. D. HAGGERTY, *op. cit.*, p. 241.

¹⁶⁵ Pour plus d'exemples, voir notamment K. D. HAGGERTY, *op. cit.*, p. 239 ; D. NELKIN & L. ANDREWS, « DNA Identification And Surveillance Creep », *Sociology of Health and Illness*, 1999, pp. 689-706 ; M. TZANOU, « The UE as an emerging surveillance society : the function creep case study and challenges to privacy and data protection », *Vienna Online J. on Int'l Const. L.*, 2010, vol. 4, pp. 407-427 ; STAFF AND AGENCIES, « Oyster data use rises in crime clamp-down », *The Guardian*, mis en ligne le 13 mars 2006, consulté le 18 mai 2016. Disponible sur : <https://www.theguardian.com/technology/2006/mar/13/news>.

¹⁶⁶ Par géolocalisation des individus et services, nous faisons référence aux pratiques commerciales visant à localiser des biens dans la chaîne de production, aux suivis des véhicules de fonction, etc.

¹⁶⁷ K. D. HAGGERTY, *op. cit.*, p. 236.

¹⁶⁸ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 9.

¹⁶⁹ *Ibid.*, p. 30.

conduite par l'impulsion d'un dessein particulier, celui de lutter et d'éradiquer tout risque potentiel inhérent au sein d'une société de plus en plus triée, classée et ciblée. Le « tri social », influencé considérablement par cette notion de risque, souligne assurément une tendance classificatrice de la surveillance moderne¹⁷⁰.

Plus précisément, les différentes pratiques de surveillance, de nature judiciaire ou commerciale, convoitent avidement les informations personnelles d'un individu ou d'un groupe dans le but de les catégoriser selon des critères divers afin de déterminer qui devrait être ciblé pour un traitement spécial, une suspicion, une admission ou une inclusion¹⁷¹. Autrement dit, une surveillance discriminatoire passe au crible une série de données pour les trier à des fins d'évaluation et de jugement. Elle est d'autant plus discriminatoire qu'elle affecte les choix de vie des individus. Si, par exemple, nous n'acceptons pas les cookies qui rapportent nos habitudes de navigation sur le net aux sociétés mères, nous pouvons alors nous attendre à ce que l'information ou l'accès ne soit plus disponible¹⁷².

La société de surveillance procède ainsi à un dernier mécanisme, celui du « tri social » des individus sur lesquels elle exerce une vigilance accrue. De surcroît, il s'agit même d'un objectif central de celle-ci, motivée par la volonté de contrôler et gérer une masse d'individus influençant, directement ou non, leurs actions¹⁷³. Une caractéristique importante, dans ce cadre, est le recours massif aux bases de données consultables – et donc au partage précédemment expliqué de celles-ci – pour obtenir une multitude de données personnelles et variées¹⁷⁴. Leur usage est, selon David Lyon, motivé par un accès rapide à de riches sources d'information sur les personnes et les populations permettant de vérifier et de surveiller le comportement, d'influencer des personnes et des populations, et d'anticiper les risques¹⁷⁵.

Dans ce qui suit, nous abordons plusieurs situations – commerciale, policière et autres à titre secondaire – en qualité d'illustration dans lesquelles le « tri social », la catégorisation et le ciblage peuvent pleinement être observés.

¹⁷⁰ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », In *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003, p. 13.

¹⁷¹ *Ibid.*, p. 20.

¹⁷² *Ibidem.*

¹⁷³ *Ibid.*, p. 1.

¹⁷⁴ Pour plus d'informations sur les bases de données, voir notamment sous-section 3.1.1., p. 43.

¹⁷⁵ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 14.

3.3.1. Première illustration : les pratiques commerciales

Le recours aux bases de données à des fins de surveillance est particulièrement frappant dans les pratiques commerciales actuelles¹⁷⁶. Tout d'abord, les consommateurs fournissent continuellement aux diverses entreprises leurs données de consommation. À chaque fois que ceux-ci payent par carte bancaire, le réseau informatique du commerce enregistre les achats et la localisation des clients. De la sorte, nous sommes de plus en plus conditionnés à accepter le fichage commercial constant de nos données personnelles sans véritablement nous questionner sur leur destin. Tout client fait partie d'une sphère commerciale de réaction évolutive qui relie leurs comportements de consommation à la collecte de données, permettant de ce fait leur classification¹⁷⁷. Les consommateurs doivent ainsi s'attendre à ce que certaines informations soient exigées de leur part dans les transactions économiques.

Ils y sont même encouragés lors de l'obtention d'une carte de fidélité ! En échange de renseignements privés que chaque acheteur fournit à la firme commerciale, ils bénéficient, en fonction de leurs habitudes de consommation, de nombreux avantages sous forme de services, cadeaux ou réductions. À l'heure actuelle, ce phénomène est en pleine expansion : nous pouvons constater que, à la fin de l'année 2006, plus de 100 millions de ces cartes étaient en circulation sur le territoire de la France métropolitaine¹⁷⁸. Un tel transfert de données permet d'affiner la catégorisation des différents clients offrant ainsi la possibilité à l'entreprise de cibler ses actions commerciales. D'ailleurs, les grandes enseignes ne s'en cachent pas, ou très peu ; le directeur général d'Auchan déclarait ainsi, en octobre 2006, que : « *Nos clients ont une relation de confiance avec nous. Nous connaissons pour chacun leur profil et leur mode de consommation, on va pouvoir leur faire des offres ciblées.* »¹⁷⁹.

Outre cet usage de données issues des diverses transactions commerciales, une large partie de l'industrie accorde également une certaine importance au regroupement de la population selon des critères géodémographiques en amont de leurs relations avec les consommateurs¹⁸⁰. Le Canada, par exemple, est organisé en différents groupes par un système informatique, le

¹⁷⁶ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 30.

¹⁷⁷ *Ibidem*.

¹⁷⁸ C.-M. VADROT, *La grande surveillance : caméras, ADN, portables, Internet...*, Paris, Seuil, 2007, p. 86.

¹⁷⁹ C. MAUSSON, « Des hypers super mobiles », *Libération*, mis en ligne le 12 octobre 2006, consulté le 10 avril 2016. Disponible sur : http://www.liberation.fr/futurs/2006/10/12/des-hypers-super-mobiles_54035.

¹⁸⁰ En économie, il s'agit traditionnellement du système de segmentation géodémographique dont la technique de classification statistique multivariée sert à classer une population en sous-groupes d'individus les plus similaires possible en appliquant plusieurs comparaisons quantitatives de caractéristiques multiples.

« Compusearch », pour ensuite être subdivisé en multiples sous-groupes¹⁸¹. Le territoire du Canada est, de la sorte, divisé en grappes allant du « U1 Urbain Affluent » au « R2 Rural Downscale ». Dans le groupe U1, nous retrouvons à titre d'exemple les élites canadiennes qui comprennent des individus, principalement concentrés dans les plus grandes métropoles du pays, dont le revenu moyen sur une année est d'un quart de million de dollars par ménage. *A contrario*, le groupe R2 concentre les habitants de petites villes ou villages qui ne perçoivent qu'un revenu modéré à hauteur de 54 000 \$ par an.

L'emploi de plusieurs bases de données liées à la localisation, à la profession et aux revenus permet, dans ce cadre, de cibler et de trier les populations selon leurs habitudes de dépenses et leur potentiel d'achat, puis de traiter les différents groupes en conséquence¹⁸². Ceux susceptibles d'être utiles aux spécialistes du marketing bénéficient d'une attention spéciale, d'offres particulières, et d'un service après-vente efficace, tandis que d'autres groupes, absents des catégories économiquement intéressantes, doivent composer avec moins d'informations et un service de qualité inférieure¹⁸³. Une telle surveillance commerciale pourrait ainsi conduire à l'exclusion ou l'absence de ciblage de personnes réputées être commercialement marginales, principalement situées en dehors des centres-villes de plus en plus embourgeoisés¹⁸⁴.

Notons enfin que des outils issus du Web ont élargi un tel processus de catégorisation pour inclure d'autres types de données, non seulement relatives à la géodémographie mais également à d'autres indicateurs de valeur¹⁸⁵. Différentes sociétés spécialisées dans la gestion et l'analyse du « Big Data » fournissent contre rémunération de multiples informations aux entreprises commerciales. Acxiom, par exemple, dont le leitmotiv consiste à exploiter la richesse des données commerciales, dispose de nombreux dossiers contenant des renseignements sur la race ou l'appartenance religieuse notamment des ménages principalement américains¹⁸⁶. Dorénavant, le vendeur peut savoir non seulement où vous vivez mais également les détails sur votre origine ethnique ou religieuse dans le but de mieux vous cibler !

¹⁸¹ http://tetrad.com/pub/documents/psyteadv_clusters.pdf, consulté le 13 mars 2016.

¹⁸² D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 14.

¹⁸³ *Ibidem*.

¹⁸⁴ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 33.

¹⁸⁵ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 14.

¹⁸⁶ M. STEPANEK, « Weblining », *Bloomberg*, mis en ligne le 3 avril 2000, consulté le 7 avril 2016. Disponible sur : <http://www.bloomberg.com/news/articles/2000-04-02/weblining>.

3.3.2. Seconde illustration : l'e-cops

Certaines pratiques policières constituent un second champ dans lequel le recours à des bases de données est devenu conséquent en matière de surveillance. En 2001, par exemple, la police canadienne de Toronto et de l'Ontario a intégré de nouveaux supports technologiques dans leurs véhicules de patrouille ayant permis d'étendre le champ des activités axées sur l'information¹⁸⁷. Dans ce cadre, l'e-Cops, acronyme d'Entreprise Case and Occurrence Processing System, a été adopté pour permettre aux patrouilles de police utilisant des ordinateurs portables de se connecter par le biais de communications sans fil à des outils informatiques pour la détection et la prévention du crime¹⁸⁸.

À l'heure actuelle, les forces de l'ordre au Canada peuvent donc accéder directement aux fichiers des services de police de Toronto, aux dossiers des permis de conduire détenus par le Ministère des Transports de l'Ontario ainsi qu'aux listes des suspects détenus au Centre canadien d'information sur la police¹⁸⁹. Non seulement les agents ont accès à toute une série de dossiers judiciaires par le biais de leurs ordinateurs portables, mais ils peuvent en outre glaner des informations extrêmement précises dans ces dossiers grâce à ce système d'e-Cops et de ses outils d'analyse¹⁹⁰.

Cette technologisation des forces de police canadiennes, comme celles des pratiques commerciales explicitées ci-dessus, utilise des données démographiques. « Dans ce cas, elle identifie les tendances géographiques des crimes et délits en vue non seulement de la détection mais également de la prévention de ces actes en indiquant où un délinquant particulier pourrait frapper »¹⁹¹. Un tel système automatise des tâches qui, auparavant, étaient plus fastueuses et isolées¹⁹². Désormais, de multiples informations générales sur les suspects sont disponibles instantanément pour ces agents en patrouille ; la base de données, accessible par le biais de leurs ordinateurs, est ainsi utilisée pour indiquer si le suspect est susceptible d'être un criminel en série ou un novice¹⁹³. Notons qu'une telle classification entre

¹⁸⁷ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 15.

¹⁸⁸ K. MARRON, « New Crime Fighter Rides Along with Cops in Cruisers », *The Globe and Mail*, mis en ligne le 23 février 2001, consulté le 8 avril 2016. Disponible sur : <http://www.theglobeandmail.com/incoming/new-crime-fighter-rides-along-with-cops-in-cruisers/article25442600/>.

¹⁸⁹ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 15.

¹⁹⁰ K. MARRON, *op. cit.*

¹⁹¹ D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 15.

¹⁹² *Ibidem.*

¹⁹³ *Ibidem.*

« délinquant prolifique » ou « délinquant amateur » est déterminée statistiquement par le nombre de condamnations sur une période donnée des individus¹⁹⁴. En conséquence, cette catégorisation par l'usage de l'e-cops fait d'un individu un candidat pour le ciblage et l'intervention policière intensive dans le cadre de la lutte contre la récidive¹⁹⁵.

3.3.3. Illustrations non-exhaustives de tri social

Le tri social, la catégorisation et le ciblage s'immiscent de manière toujours plus importante dans la réalité quotidienne de notre société. Un tel processus est un phénomène rampant dont il n'est toutefois pas aisé d'en dresser une liste exhaustive des facettes sociales dans lesquelles il s'inscrit insidieusement. Dans cette dernière sous-section, nous souhaitons examiner deux autres situations pour souligner sa portée universelle.

Le climat des préoccupations sécuritaires accrues aux frontières intensifie la tendance au « tri social » aux différents points de passage territoriaux. Il est ainsi couramment exigé, lorsqu'un voyageur étranger souhaite pénétrer sur le territoire des États-Unis, une vérification méticuleuse de l'identité de celui-ci au même titre qu'une authentification précise de ses activités. L'objectif déclaré est de pouvoir, par la collecte de toute une série de données personnelles, contrôler et trier l'ensemble des individus qui entrent sur le territoire.

En outre, à de nombreux points d'entrée maritime, aérienne ou terrestre, il est devenu commun de voir des voies rapides pour traverser la frontière¹⁹⁶. La méthode « Privium » de l'aéroport d'Amsterdam Schiphol aux Pays-Bas illustre parfaitement cette tendance. Présenté comme un service pour les voyageurs fréquents qui souhaitent se déplacer sans heurts, ce programme offre des avantages exclusifs qui assurent rapidité, confort et priorité lors du voyage en contrepartie de la soumission du passager à un scan de l'iris¹⁹⁷. Outre les traditionnelles questions relatives à la vie privée, de telles pratiques entraînent un véritable tri des voyageurs en catégories de risque qui justifie l'application de mesures plus importantes de surveillance pour ceux qui ne souhaitent ou ne peuvent profiter de cette voie rapide¹⁹⁸.

¹⁹⁴ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 33.

¹⁹⁵ *Ibidem*.

¹⁹⁶ *Ibid.*, p. 31.

¹⁹⁷ Ce programme offre un passage rapide du contrôle à la frontière, des places de parking avantageuses, des réductions avec toute une série de partenaires liés à l'aéroport, un accès à des espaces de bien-être et ainsi de suite. Voy : <http://www.schiphol.nl/Travellers/AtSchiphol/Privium.htm>.

¹⁹⁸ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 31.

Le système de carte d'identité proposé en Grande-Bretagne s'inscrit dans la même veine. Il aurait, par exemple, la capacité de trier ceux qui sont admissibles aux services et aux différents accès sociaux, médicaux ou judiciaires, et les autres¹⁹⁹. Nous pouvons craindre avec cette illustration que des mécanismes invisibles biaisent le système à l'encontre de ceux qui sont déjà susceptibles d'être désavantagés, par la volonté de réglementer ou de restreindre les activités des personnes indésirables ou désignées comme étant non admissibles²⁰⁰. Cette possibilité de s'engager à long terme, grâce à ces cartes, dans un tri social constant est bien plus insidieuse que la crainte d'une réduction de la mobilité lorsque des papiers d'identité sont exigés. Selon l'association caritative « Surveillance Studies Network », « ce tri social tend à produire une citoyenneté de seconde classe plutôt que de soutenir une pratique plus solidaire et égalitaire »²⁰¹.

La surveillance, comprise comme étant une vigilance systématique envers les données personnelles, procède clairement au tri social et au ciblage comme mécanisme au sein de la société de surveillance à l'instar du partage de l'information et du détournement d'usage. Certes la catégorisation est endémique et nécessaire pour la vie sociale²⁰². Toutefois, en fonction des risques que représente un groupe d'individus particuliers, les pratiques discriminatoires d'une surveillance accrue tendent à reproduire et à accentuer les inégalités sociales au sein de la société dans une volonté de contrôle et de gestion de ce groupe. L'ensemble de la société, sans délimitation spatiale, se retrouve en partie déterminée par le « tri social ». La catégorisation est ainsi un phénomène global qui n'est pas limité aux secteurs commerciaux et judiciaires ! Nous observons finalement un tel processus dans divers secteurs là où, *in fine*, des pratiques de surveillance sont à l'œuvre.

¹⁹⁹ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 31.

²⁰⁰ D. LYON, « Identity cards : social sorting by database », *Oxford Internet Institute, Internet Issue Brief No. 3*, 2004, p. 7.

²⁰¹ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 31.

²⁰² D. LYON, « Surveillance as social sorting : computer codes and mobile bodies », *op. cit.*, p. 21.

4. Les nouvelles technologies de surveillance

Au sein de la société de surveillance, de nombreux mécanismes sont à l'œuvre²⁰³. Pour contrôler, gérer et influencer un groupe d'individus, les autorités étatiques et leurs services procèdent à un détournement d'usage et à un tri social dont l'aboutissement est, en partie, subordonné à un partage considérable de l'information. Cependant, la mise en œuvre et le développement de ces mécanismes dépendent grandement des nouvelles technologies dont le rôle fondamental permet d'améliorer la collecte de renseignements, l'identification et le traçage des individus. « La société actuelle se développe autour de nombreuses technologies de l'information et de la communication disposant de la capacité de recueillir, de stocker et de traiter de grandes quantités de données pour la sauvegarde de la sécurité »²⁰⁴. Alors qu'il est vital de ne pas oublier l'importance d'une surveillance non-technologique, il est incontestable que les nouvelles technologies ont contribué à changer la nature de la surveillance²⁰⁵. L'usage de ces dispositifs technologiques par les juges d'instruction et les services de police au sein des arrondissements judiciaires en Wallonie constitue le sujet central de ce chapitre.

La technologie est ainsi au cœur de la société de surveillance. Qu'entendons-nous par « nouvelle technologie » ? Selon le dictionnaire Larousse, ce terme fait référence aux savoir-faire pratiques et à l'utilisation d'outils qui mettent en œuvre les découvertes et les applications scientifiques les plus récentes. Cette définition recouvre un champ d'application extrêmement vaste. Pour éviter de noyer le lecteur de ces lignes, nous avons dès lors choisi de délimiter notre recherche à l'étude des instruments de traçabilité.

Dans ce cadre, nous avons divisé ce chapitre en trois sections. La première est consacrée à l'étude individuelle des technologies numériques de traçabilité. Plus précisément, nous analysons le mécanisme et l'apport, dans une enquête pénale, du téléphone portable – de la carte bancaire – et de la base de données commerciales. De tels propos nous permettent ensuite d'aborder deux interrogations majeures : selon quels critères et dans quel type d'enquête ces moyens sont-ils mobilisés ? L'usage général de ces technologies par les acteurs judiciaires constitue ainsi la deuxième section de ce chapitre. La dernière section aborde enfin le principe de la synergie technologique selon lequel un tel usage des instruments de traçabilité s'inscrit dans un ensemble de méthodes particulières d'enquête.

²⁰³ Voy. Chapitre 3, p. 41.

²⁰⁴ M. TZANOU, « The UE as an emerging surveillance society : the function creep case study and challenges to privacy and data protection », *Vienna Online J. on Int'l Const. L.*, 2010, vol. 4, p. 409.

²⁰⁵ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 17. Voy. Section 2.5. p. 28 & Sous-section 2.2.1. p. 36.

4.1. Les technologies numériques de traçabilité

La traçabilité des individus désigne la possibilité de suivre des trajectoires à partir des traces numériques abandonnées sur leur passage dans tous les lieux réels et virtuels de la société contemporaine. Ces traces sont créées et collectées non plus par l'homme mais par des technologies aussi diverses que variées. Il s'agit d'une nouveauté importante dans la société de surveillance. Les personnes sont désormais traçables, presque intégralement, grâce aux cartes bancaires, aux cartes de fidélité, aux caméras de vidéosurveillance, aux téléphones portables qui laissent des marques durables de nos actes et de nos déplacements²⁰⁶. Pour autant, rares sont celles qui ont connaissance que leurs activités engendrent une quantité considérable de données. Une explication plausible de cette ignorance serait liée au fait que la traçabilité et ses mécanismes soient généralement mal perçus par l'opinion publique, ceci en partie dû au caractère ambivalent de ces nouvelles technologies. Avant d'aborder en détail les technologies numériques de traçabilité, nous estimons donc opportun de présenter, de manière générale, un tel caractère.

Vincent Francis, interrogé dans le cadre de notre recherche, estime que les technologies numériques se différencient en fonction de leur finalité. Il distingue ainsi deux catégories ambivalentes d'instruments en matière de traçabilité, certaines sont des technologies sécuritaires alors que d'autres sont des technologies de confort.

« Vous avez tout d'abord les instruments conçus avec une finalité sécuritaire. La vidéosurveillance est un instrument de traçabilité. C'est un dispositif qui permet de laisser des traces et de les récolter. Il y a l'enregistrement qui est au fond une trace numérique tout à fait exploitable et qui n'existe que parce qu'on a pensé un dispositif capable de produire des traces numériques. Là c'est un dispositif dont la première fonction est sécuritaire »²⁰⁷.

La première catégorie regroupe ainsi les instruments de traçabilité numérique dont la fonction première a trait à la sécurité. Nous y retrouvons principalement la vidéosurveillance. À titre illustratif, les caméras de vidéosurveillance consacrées à la reconnaissance automatique des plaques sont des outils capables de lire des plaques minéralogiques et d'enregistrer les allées

²⁰⁶ C. LAVAL, *op. cit.*, p. 65.

²⁰⁷ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

et venues des personnes²⁰⁸. Dans le but de pouvoir identifier le conducteur d'un véhicule, ce dispositif crée et récolte d'abord une trace pour ensuite être prioritairement exploitée à des fins de prévention de certaines infractions. « Ces caméras ANPR sont un autre exemple d'une technologie purement sécuritaire au départ »²⁰⁹. En conséquence, la mise en place et le développement de cet instrument de traçabilité sont motivés, à l'origine, par des objectifs sécuritaires.

« A coté de cela vous avez ensuite d'autres dispositifs qui n'ont jamais été pensés au départ à des fins sécuritaires. Ce sont les technologies de confort qui sont apparues dans les années 1990. On pense au téléphone portable, au GPS,... On peut aussi y regrouper tout ce qui est puce RFID. Ce sont des puces qui émettent à distance, à quelques mètres seulement. Tout cela a été pensé pour la gestion des stocks, le suivi des marchandises, des objets ou personnes. Les technologies de confort n'ont pas été pensées à des fins sécuritaires mais vont pouvoir être, à titre secondaire, exploitées à des fins sécuritaires »²¹⁰.

La seconde catégorie regroupe donc les technologies de confort dont la fonction première est liée aux pratiques commerciales ou à l'usage personnel. Elles ne sont qu'accessoirement mobilisées pour rencontrer des objectifs sécuritaires. Pour illustrer ce genre de technologies, nous pouvons tout d'abord évoquer le téléphone portable. Un gsm est avant tout un bien utilitaire pour les consommateurs. Ce n'est qu'accessoirement qu'il est utilisé à des fins de surveillance par les services de police et de renseignement. De nombreuses autres technologies se retrouvent également sous cette catégorie particulière : le gps, les cartes de transport utilisées par les usagers, les cartes de fidélité et les cartes de crédit, les bases de données à vocation commerciale, etc. Toutes poursuivent des finalités commerciales pouvant également avoir une exploitation sécuritaire. Autrement dit, l'objectif est de « *pouvoir utiliser, et c'est déjà envisagé par les responsables de la sécurité, un certain nombre de dispositifs qui ont d'autres finalités mais qui vont pouvoir produire un certain nombre de traces exploitables d'un point de vue sécuritaire* »²¹¹.

²⁰⁸ Pour plus d'informations, voir notamment <https://www.besafe.be/fr/base-de-connaissance/anpr-un-r-seau-cam-ras-surveillance-et-lecteurs-plaques-d-immatriculation-aide->.

²⁰⁹ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²¹⁰ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²¹¹ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

Le recours aux technologies de confort est une véritable innovation en matière de contrôle et de sécurité. Pour la première fois, des personnes susceptibles à un moment donné de devoir être soumises à une enquête judiciaire sont amenées à produire par elles-mêmes leurs propres traces en l'absence de dispositifs externes de surveillance. Comme nous l'avons expliqué à la section 2.5. relative aux économies de l'information personnelle, nous produisons nous-mêmes les traces qui vont permettre de nous tracer et de nous surveiller. Vincent Francis estime que *« c'est beaucoup plus puissant que les dispositifs qui ont directement été créés dans le but de nous surveiller. Nous laissons beaucoup plus de traces numériques dans le cadre de nos activités routinières que celles que nous laissons parce que l'on passe devant des dispositifs, comme une caméra de vidéosurveillance, pensés à des fins sécuritaires »*²¹². L'utilisation du gsm, des cartes à puce, de l'ordinateur ou du gps génère ainsi une quantité phénoménale de données éminemment supérieure à celle émise par des dispositifs de surveillance. *« C'est incroyable le nombre de traces que nous abandonnons dans notre sillage. Nous ne restons pas une heure sans laisser de traces en raison de l'usage des ces biens de confort laissant derrière nous de larges traînées numériques »*²¹³. Une telle profusion de données favorise en conséquence une surveillance de plus en plus importante par les services de police et de renseignement à partir de ces technologies de confort.

Suite à ces considérations générales, nous souhaitons approfondir plusieurs technologies numériques de traçabilité. Parmi cet ensemble considérable, nous analysons plus particulièrement trois instruments particuliers : la téléphonie mobile – la carte bancaire – et la base de données commerciales.

4.1.1. La téléphonie mobile

La surveillance par la téléphonie mobile désigne la capacité de contrôler et de stocker l'information relative au contenu, à la localisation et à la fréquence des télécommunications échangées entre plusieurs individus²¹⁴. À cet égard, les développements technologiques en matière de téléphonie mobile ont permis d'accroître les capacités de surveillance par les autorités étatiques²¹⁵. La position d'un appareil téléphonique peut ainsi être déterminée, dans le cadre restreint de la traçabilité, par le repérage du signal émanant de l'appareil et la

²¹² Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²¹³ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²¹⁴ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 17.

²¹⁵ *Ibidem*.

réception de celui-ci auprès d'un certain nombre d'antennes-relais. C'est dans cette lignée que le Code d'instruction criminelle implante, dans le droit belge, une telle pratique « lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité »²¹⁶. Porter sur soi un téléphone génère donc des traces et des informations de déplacement susceptibles d'informer des tiers de nos mouvements et de nos activités²¹⁷.

Le téléphone portable offre ainsi une nouvelle dimension à la surveillance : la géolocalisation ou la traçabilité à tout moment donné d'un terminal téléphonique. Toutefois, ces propos introductifs ne permettent pas de répondre pleinement à une question fondamentale de notre recherche : comment les services de police parviennent-ils à tracer les mouvements d'un individu dans le cadre d'une enquête judiciaire ? Pour évaluer cette possibilité de surveillance, il est nécessaire de procéder à une description approfondie de la manière dont un téléphone portable est relié au réseau de téléphonie mobile. En effet, l'appareil téléphonique peut être géolocalisé lorsqu'il communique pour diverses raisons avec la structure du réseau cellulaire. La première partie des développements sur la téléphonie mobile est par conséquent consacrée à cette description.

4.1.1.1. Téléphone portable et réseau cellulaire

Le système de radiotéléphonie en Belgique se base sur une liaison radioélectrique entre les téléphones portables et le réseau cellulaire. Celle-ci est fondamentale pour assurer une télécommunication, prise en charge par un opérateur téléphonique, entre deux individus. Pour ce faire, la liaison radioélectrique entre le téléphone et le réseau doit notamment être de qualité suffisante, ce qui nécessite la mise en place d'un certain nombre d'antennes-relais sur l'ensemble du territoire que l'on souhaite couvrir. C'est le principe de base à l'heure actuelle en matière de téléphonie mobile.

Plus précisément, l'antenne-relais est un émetteur-récepteur de signaux radioélectriques dont l'objectif principal est d'acheminer les communications électroniques dans une zone géographique. Les différents opérateurs de réseau mobile ont ainsi investi dans l'installation

²¹⁶ Art. 88bis, § 1 du Code d'instruction criminelle.

²¹⁷ C. LEVALLOIS-BARTH, « La géolocalisation : un nouvel impératif », *Hermès, La Revue*, 2009, vol. 1, p. 99.

de nombreuses antennes téléphoniques, représentées sous la forme de points fléchés dans le schéma de la page 71, réparties sur la totalité du territoire. Frédéric Pierard, ingénieur à l'Institut belge des services postaux et des télécommunications, explicite, lors d'un entretien mené dans le cadre de notre recherche, le fondement de ces antennes. « *Sur une borne téléphonique, nous retrouvons généralement trois émetteurs-récepteurs de 120 degrés chacun ayant pour but de couvrir la circonférence d'une antenne. Cette dernière va ainsi rayonner sur une zone de couverture et y acheminer une communication* »²¹⁸. Jean-Yves Deloyer, inspecteur principal à la Police Judiciaire Fédérale de Namur, confirme ces propos dans un entretien : « *Installées pour recouvrir un territoire donné, les antenne-relais émettent plusieurs zones de couverture qui s'étendent autour de la circonférence de leur pylône* »²¹⁹.

Les zones de couverture d'une antenne émises par les émetteurs-récepteurs sont plus communément appelées « cellules ». Ce terme désigne une aire géographique, représentée sous une forme hexagonale ci-dessous, dans laquelle le téléphone portable établit une liaison radioélectrique avec une borne téléphonique déterminée. Jean-Yves Deloyer confirme ce postulat général. « *Généralement, nous retrouvons trois cellules attachées à un pylône. Chaque cellule est caractérisée par un numéro (1, 2, 3). Sauf lorsqu'il est éteint, le téléphone portable d'un individu est toujours lié à une borne et à sa cellule permettant de se connecter au réseau téléphonique* »²²⁰. Frédéric Pierard corrobore cette description en ajoutant que « *chaque téléphone allumé est en permanence connecté au réseau cellulaire par son attachement à une cellule. Vous êtes toujours, quand votre GSM est allumé, connectés sur une antenne-relais.* »²²¹. Il s'agit d'un fondement essentiel pour que « *l'opérateur sache où vous êtes afin de pouvoir acheminer un appel* »²²². Le principe consiste à ainsi diviser une région en un certain nombre de cellules contiguës et desservies par une même borne pour connecter un téléphone portable au réseau cellulaire et permettre l'échange des télécommunications.

Sur le plan individuel, les cellules ont un rôle essentiel en téléphonie mobile en assurant la connexion du téléphone portable au réseau cellulaire. Toutefois, elles ne peuvent à elles seules parvenir à se gérer. C'est pourquoi une entité de cellules regroupant plusieurs pylônes se constitue pour former un dernier élément constitutif du paysage téléphonique : le Local

²¹⁸ Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

²¹⁹ Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

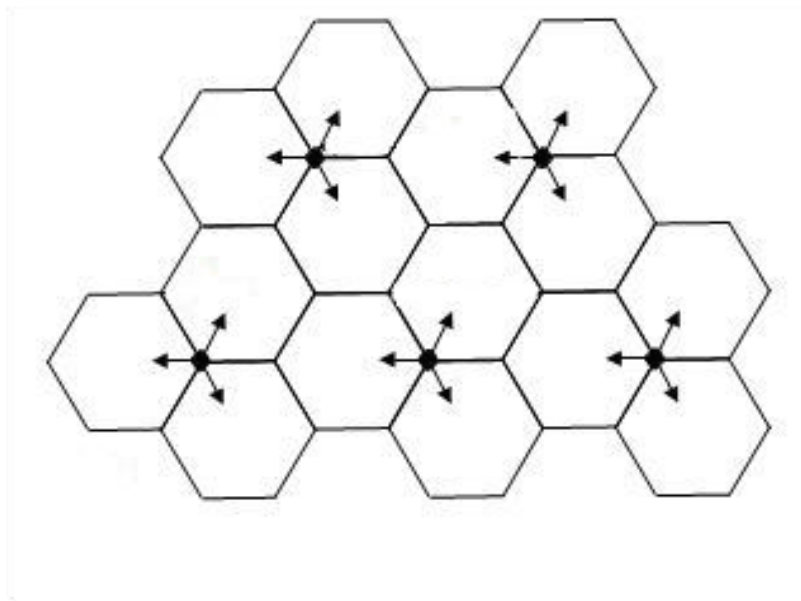
²²⁰ Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

²²¹ Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

²²² Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

Area Code. Erik Kindt, membre de la Cellule de coordination avec la Justice chez Proximus, nous décrit brièvement ce que représente un « Local Area Code ». *« La Belgique est divisée en une multitude de LAC. Il s'agit d'un ensemble contigu de cellules. On peut le visualiser comme une ruche d'abeilles. Dans un LAC nous retrouvons un certain nombre d'antennes téléphoniques à partir desquelles émanent des cellules »*²²³. Jean-Yves Deloyer précise ces propos : *« Un LAC est un petit serveur qui gère plusieurs pylônes et la densité des appels sur le territoire couvert. Il peut rediriger les communications électroniques lors de saturation sur d'autres pylônes. Le LAC gère ainsi le trafic d'appels et de communications »*²²⁴. Si la fonction organisationnelle du Local Area Code nous intéresse peu dans le cadre de notre recherche, celui-ci joue toutefois un rôle important dans la géolocalisation d'un téléphone portable que nous présentons dans la seconde partie des développements qui suivent.

Ci-dessous, nous avons souhaité reproduire par nos soins un schéma dans le but d'illustrer ces propos. Celui-ci représente un Local Area Code composé d'antennes-relais couvrant par des cellules un territoire particulier. Notons que les opérateurs téléphoniques ont généralement recours à l'hexagone pour penser théoriquement leur réseau cellulaire ; hexagone dont la forme régulière peut se juxtaposer sans laisser de zones vides. Toutefois, la réalité du terrain peut s'avérer légèrement différente de ce modèle théorique, notamment en zone urbaine où de nombreux obstacles empêchent une propagation linéaire.



²²³ Entretien avec Monsieur Erik Kindt réalisé le 5 février 2016.

²²⁴ Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

Tout téléphone portable s'inscrit donc dans un complexe réseau cellulaire dont nous avons tenté d'esquisser les principaux traits. Cette description est un prélude nécessaire pour comprendre comment celui-ci peut être géolocalisé. En effet, des notions théoriques comme l'antenne téléphonique, la cellule et le Local Area Code interagissent avec le téléphone et participent ainsi à sa localisation. Nous abordons désormais avec ces acquis ce mécanisme. La géolocalisation d'un téléphone constitue de la sorte la seconde partie de ces développements sur la téléphonie mobile.

4.1.1.2. La géolocalisation d'un téléphone portable

La géolocalisation d'un téléphone portable est, avant toute chose, effectuée par les opérateurs de téléphonie mobile en considération de motifs pratiques et économiques : pour acheminer un appel, encore faut-il pouvoir localiser les téléphones concernés. Ainsi, ils peuvent aisément déterminer par des moyens techniques la localisation de leurs clients. Pour rencontrer des objectifs sécuritaires et juridiques, les services de police ont fréquemment recours à cette opportunité offerte, en vertu de l'obligation de rétention et de collaboration explicitée au point 3.1.2.3., par ces sociétés selon les besoins de l'enquête judiciaire. De cette façon, la police dispose de plusieurs procédés pour parvenir à géolocaliser et à tracer un téléphone portable. Erik Kindt nous énonce le principe de base : *« lorsque un appareil mobile est allumé, celui-ci est en connexion continue avec le réseau par une communication quotidienne entre l'appareil en question et l'antenne. Cette communication est enregistrée dans les bases de données de l'opérateur, ce qui permet de déterminer la localisation de ce contact et, dès lors, de l'individu »*²²⁵. La traçabilité d'un téléphone est, par conséquent, subordonnée aux communications électroniques, entre ce terminal téléphonique et le réseau cellulaire, dont les formes particulières sont multiples et empruntent notamment celles d'un appel, de messages ou d'un changement de Local Area Code.

Il existe plusieurs méthodes mobilisées par les services de police pour géolocaliser et tracer un téléphone portable. Suite aux entretiens effectués dans le cadre de notre recherche, nous avons pu distinguer deux formes distinctes de géolocalisation : la géolocalisation rétroactive et la géolocalisation en temps réel. Nous procédons à leur présentation dans la suite de ces développements.

²²⁵ Entretien avec Monsieur Erik Kindt réalisé le 5 février 2016.

La géolocalisation rétroactive désigne la faculté de déterminer les mouvements d'un individu particulier dans une période de temps écoulée. Cette traçabilité se base nécessairement sur une pluralité de communications électroniques dont l'échange active les antenne-relais les plus proches du téléphone portable permettant dès lors de situer cet appareil dans les cellules couvertes par les bornes²²⁶. Jean-Yves Deloyer aborde la géolocalisation rétroactive en ces termes : « *Si on veut tracer le chemin d'un individu, on se base sur les données transmises par le gsm au réseau téléphonique par le biais de pylônes indiquant l'endroit où la communication, et donc l'individu, se situe* »²²⁷. Stéphane Kerkhofs, juge d'instruction à Liège, énonce le même principe lors d'un entretien mené dans le cadre de notre recherche. « *Il peut y avoir une géolocalisation rétroactive d'un individu sur base d'un Call History où l'on voit apparaître les pylônes activés par un suspect qui téléphone ou envoie des sms. À partir des pylônes bornés, on peut déterminer au niveau des cellules la localisation et les déplacements effectués par l'individu* »²²⁸.

Si la géolocalisation rétroactive se fonde sur les communications émises ou reçues par une personne, ces dernières doivent assurément être enregistrées dans les bases de données de l'opérateur au sein desquelles figure notamment la localisation des échanges. La communication et son enregistrement constituent ainsi les piliers sur lesquels elle repose. Comme l'affirme Christine Dierick, juge d'instruction à Tournai, « *cette géolocalisation est transmise à la police lorsque les opérateurs déterminent à la suite d'une demande de la justice l'historique des appels entrant ou sortant enregistrés* »²²⁹. À partir de ces échanges électroniques et de leurs enregistrements, les services de police, avec la collaboration des opérateurs téléphoniques, déterminent donc plus ou moins précisément les mouvements et déplacements effectués par un particulier dans une période temporelle écoulée.

Tel est le principe de base de la géolocalisation rétroactive. Toutefois, dans le cadre de cette première méthode de traçabilité téléphonique, une question demeure en suspens. Quelle est la précision d'une telle localisation ? Celle-ci dépend de l'antenne-relais. Il en existe de différentes sortes sur le territoire couvert par l'opérateur. Frédéric Pierard établit le postulat suivant : « *Nous pouvons constater des pylônes qui émettent des cellules ayant une couverture importante ; aux alentours de cinq kilomètres comme c'est le cas en campagne. A contrario, nous pouvons également observer des pylônes dont la portée de la cellule est limitée,*

²²⁶ C. DE VALKENEER, *Manuel de l'enquête pénale*, 4^e éd., Bruxelles, Larcier, 2011, p. 357.

²²⁷ Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

²²⁸ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²²⁹ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

notamment sur la Grand-Place de Bruxelles, à une centaine de mètres »²³⁰. Ainsi, la couverture de la cellule est plus ou moins importante selon la densité et le flux de la population sur un territoire particulier. « En fonction du type d'antenne, la couverture de cette antenne varie et ce que l'on donne comme information de localisation aux services de police est plus ou moins précis, restreint ou large »²³¹. Par conséquent, au plus la couverture de la cellule est importante, au moins la géolocalisation est précise. Il est dès lors nécessaire d'être prudent dans l'étude des déplacements effectués par un individu. Pour éviter d'aboutir à des conclusions erronées, il importe selon Jean-Yves Deloyer :

« D'étudier une période temporelle large afin d'avoir le plus de communications possibles dans le but de déterminer avec précision les déplacements effectués. Nous ne pouvons aboutir à des conclusions correctes avec l'exploitation téléphonique au niveau localisation en ne regardant qu'une communication. Autrement dit, il est nécessaire d'observer un nombre important d'échanges téléphoniques permettant d'interpréter au mieux les mouvements et déplacements des individus »²³².

La géolocalisation rétroactive présente d'indéniables avantages. Il peut ainsi être intéressant de déterminer les allées et venues d'un suspect avant – pendant – et après la commission d'une infraction afin de le disculper, ou non, des faits qui lui sont reprochés. Toutefois, les autorités judiciaires doivent également dans l'exercice de leurs fonctions, selon les spécificités de l'enquête judiciaire, pouvoir suivre en temps réel les mouvements de certaines personnes. Les services de police bénéficient dès lors d'une seconde méthode de traçabilité téléphonique : la géolocalisation en temps réel.

La géolocalisation en temps réel par le biais de la téléphonie mobile désigne quant à elle la possibilité de suivre présentement une personne et son téléphone portable à son insu lorsque les nécessités de l'enquête l'exigent. « Il peut y avoir une géolocalisation en temps réel où l'on se trouve à un niveau beaucoup plus intrusif que le simple relevé des communications pour obtenir la localisation passée d'un individu »²³³. Cette méthode particulière d'enquête est basée non plus sur les communications échangées mais sur le changement du Local Area

²³⁰ Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

²³¹ Entretien avec Monsieur Jean-François Vergieu réalisé le 10 février 2016.

²³² Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

²³³ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

Code. Frédéric Pierard en explicite l'essence : « *Quand on passe d'une cellule à l'autre, l'opérateur ne va pas notifier ce mouvement. Toutefois, lorsqu'on passe d'un LAC à l'autre, il va enregistrer ce déplacement pour des raisons techniques. Dès lors, si l'on part de Tournai pour se rendre à Liège, l'opérateur va enregistrer la traversée des différents LAC.* »²³⁴. L'opérateur téléphonique connaît par conséquent les déplacements de ses clients par le biais des différents Local Area Code traversés. Grâce à la collaboration entre les entreprises de téléphonie et les autorités judiciaires, précédemment explicitée, les services de police vont pouvoir, de ce fait, recevoir les informations nécessaires pour localiser un individu. « *L'opérateur donne à la police par simple ordonnance l'accès, par ordinateur, à toutes leurs données. Nous pouvons ainsi observer où se trouve la personne par le signal du LAC qui est envoyé* »²³⁵. Dès lors, la police bénéficie assurément d'une véritable méthode pour géolocaliser en temps réel certaines personnes. « *La géolocalisation n'est pas un mythe ; il est, en effet, possible de voir que l'individu a traversé plusieurs LAC différents, ce qui permet d'apprécier précisément le cheminement effectué en fonction d'un itinéraire logique de déplacement, la vitesse de l'individu et les bornes activées* »²³⁶.

En conséquence, la traçabilité des individus par la téléphonie mobile est loin d'être une illusion fictive et abstraite au sein des enquêtes policières. Ces pratiques de surveillance dont nous avons esquissé le fonctionnement de base constituent de véritables méthodes d'enquête. Sont-elles pour autant mobilisées fréquemment par les autorités judiciaires ? Intimement liée à celle de la fréquence, la question des frais engendrés mérite également d'être posée. Quel est le coût financier de ces demandes de traçabilité téléphonique pour la justice ? La fréquence et le coût de la géolocalisation téléphonique constituent enfin la dernière partie de nos propos sur la téléphonie mobile.

4.1.1.3. La fréquence et le coût de la géolocalisation téléphonique

Quelle est la place de la traçabilité téléphonique dans la conduite d'une enquête judiciaire en Wallonie ? Cette interrogation essentielle mérite d'être posée aux professionnels de la justice et des services de police. Celle-ci a pour objectif, à l'aune de leurs réponses, d'apprécier l'ampleur de la géolocalisation téléphonique dans les pratiques de la justice pénale.

²³⁴ Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

²³⁵ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²³⁶ Entretien avec Monsieur Frédéric Pierard réalisé le 9 novembre 2015.

A la question de savoir si cette faculté de surveillance est fréquemment utilisée, toutes les personnes interrogées dans le cadre de nos entretiens ont répondu par l'affirmative. Martine Michel résume parfaitement les propos recueillis auprès des juges d'instruction lors des entretiens : *« Oui, je l'utilise extrêmement fréquemment dans tout type de dossier. J'y suis familière au niveau de l'utilisation. Cette technique de localisation est évidemment chez nous un sujet important : voir les déplacements d'une personne près d'une scène de crime. C'est important de le savoir et donc c'est une technique extrêmement utilisée »*²³⁷. Nous avons observé le même constat auprès des services de police : *« On a souvent recours à la téléphonie dans le cadre de nos enquêtes »*²³⁸. En outre, il ressort clairement des entretiens effectués un usage toujours plus important de la géolocalisation téléphonique en raison des renseignements que cette dernière confère aux autorités judiciaires. David Cruyplandt, membre de la « Cellule coordination Justice » chez Mobistar, nous confirme cette augmentation lors d'un entretien : *« chaque année, il y a une hausse. Ca s'est stabilisé un peu ces dernières années mais il y a encore une hausse de 7% par rapport à l'année 2014 »*²³⁹.

À travers l'analyse des coûts financiers relatifs aux requêtes en traçabilité téléphonique, nous pouvons également apprécier, sous un autre angle, l'augmentation sensible affirmée par David Cruyplandt. Avant d'aborder en détail les montants alloués à la géolocalisation par la justice pénale, il convient tout d'abord de mentionner le principe budgétaire de base en matière de téléphonie mobile. *« Par service et mission demandés auprès des opérateurs téléphoniques, il y a un coût prévu par un arrêté royal. Ce coût n'est donc pas inventé par l'entreprise même s'il évolue en fonction des interventions du législateur »*²⁴⁰. Ainsi, l'ensemble des services offerts par les opérateurs téléphoniques est tarifé selon les indications du gouvernement dans les différents Arrêtés Royaux successifs. *« Les tarifs plusieurs fois modifiés sont présents dans l'actuel Arrêté Royal et ce sont les acteurs étatiques qui les ont fixés »*²⁴¹. Dès lors, il est nécessaire de se référer au texte légal actuellement en vigueur pour mesurer les frais de justice dans le cadre de la téléphonie mobile. À titre illustratif, la totalité des coûts de la justice pénale, non-limités à la traçabilité des téléphones portables, est estimée *« autour des 20 millions d'euros par année pour l'ensemble des opérateurs »*²⁴².

²³⁷ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

²³⁸ Entretien avec Monsieur Jean-Yves Deloyer réalisé le 27 avril 2016.

²³⁹ Entretien avec Monsieur David Cruyplandt réalisé le 4 mars 2016.

²⁴⁰ Entretien avec Monsieur Erik Kindt réalisé le 5 février 2016.

²⁴¹ Entretien avec Monsieur Jean-François Vergieu réalisé le 10 février 2016.

²⁴² Entretien avec Monsieur David Cruyplandt réalisé le 5 février 2016.

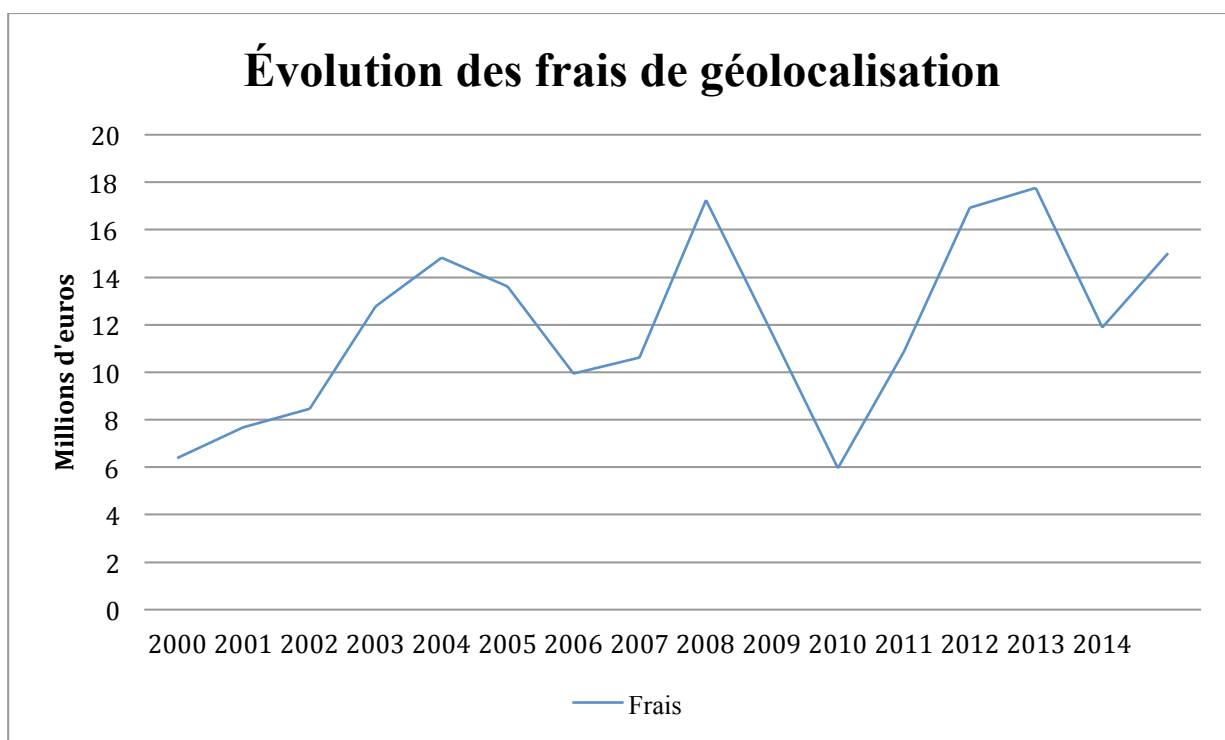
Qu'en est-il plus particulièrement des coûts pour la géolocalisation ? Il est nécessaire, dans un premier temps, de s'attarder sur les tarifs prévus à l'heure actuelle pour la seule demande de géolocalisation. Ceux-ci sont fixés de la manière suivante dans l'annexe de l'arrêté royal du 8 février 2016 modifiant celui adopté le 9 janvier 2003 :

« Art. 2. Collaboration légale indemnisée par prestation

A. Observation en temps réel ; quelle que soit la durée et indépendamment d'éventuelles prolongations : 92 euros par demande.

B. Observation de données historiques (rétro-observation) ; quelle que soit la période demandée : 80 euros par demande »²⁴³.

Après avoir brièvement mentionné le coût financier pour une demande de géolocalisation, il nous paraît opportun, dans un second temps, de s'attarder sur les frais globaux liés à l'ensemble de ces demandes. Quels sont les montants alloués par la justice pénale et leur évolution en matière de traçabilité téléphonique ? Se basant sur les données de la Commission de Modernisation de l'Ordre Judiciaire, nous avons pu établir l'évolution des frais de géolocalisation depuis l'année 2000 jusqu'en 2014 dans le graphique suivant²⁴⁴.



²⁴³ Art. 2, § 1 de l'annexe de l'Arrêté Royal du 8 février 2016 modifiant l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

²⁴⁴ Source: Commission de Modernisation de l'Ordre Judiciaire, consulté le 3 avril 2016.

Comme nous pouvons l'observer à la faveur de ce graphique, les frais de géolocalisation croissent sensiblement au fil des années. Ce constat est particulièrement visible entre l'année 2000 et l'année 2008 ; période au sein de laquelle les frais de justice pour les requêtes de géolocalisation évoluent respectivement de 6 388 311€ à 17 260 847€. Certes, après cette période, ceux-ci connaissent une baisse nette et atteignent lors de l'année 2010 un plancher inédit de 5 956 856€. Nous observons, cependant que s'ensuit à nouveau un accroissement continu et constant pour culminer dans le courant de l'année 2013 à un sommet de 17 772 157€. Pour notre part, nous estimons que ces variations peuvent être liées soit à la fréquence même du recours à ces méthodes, ce qui nous semble prédominant, soit aux frais eux-mêmes soumis à une certaine fluctuation et imposés par les autorités publiques aux opérateurs privés pour leur emploi. En définitive, les montants alloués par la justice sont considérables. « *C'est 1/3 du budget de la justice qui passe dans ces factures de téléphonie* »²⁴⁵.

De telles données appellent certaines questions qui, dans un contexte budgétaire toujours plus interpellant, semblent nécessaires. Assurément, ces méthodes de géolocalisation ont prouvé leur nécessité et leur utilité, notamment au cours des dernières années avec l'essor des activités terroristes sur le territoire européen. Toutefois, les décisions budgétaires et leurs contradictions avec les besoins des services publics en matière de justice et de sécurité se sont invitées dans le débat public et la contestation sociale, et sont aujourd'hui plus brûlantes que jamais. Loin de nous l'idée de poser un jugement politique par essence sur la gestion des services publics et l'utilisation du budget qui leur est alloué ; néanmoins, n'y a-t-il pas moyen d'agir sur les deux facteurs que nous avons mentionnés, soit par un encadrement plus strict et supervisé du recours aux moyens de géolocalisation, soit en renégociant les tarifs actuels auprès des opérateurs de télécommunication, afin de réduire la charge que représentent ces montants sur le budget de la justice ? Sans préjudice des propositions demandant un refinancement du service public, ces pistes devraient selon nous être explorées.

4.1.2. La carte bancaire

La traçabilité des individus n'est pas exclusivement fondée sur les communications émises par un téléphone portable via le réseau cellulaire ; elle existe également au niveau de l'appareil bancaire et de l'ensemble des transactions économiques qui prennent place à

²⁴⁵ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

l'intérieur du système financier international. À cet égard, toute opération financière – qu'il s'agisse d'un achat par carte de paiement, d'un retrait dans une banque ou d'un virement entre particuliers – laisse une trace identitaire et informationnelle à propos de son auteur. Comment l'expliquer ? Au même titre qu'en matière de téléphonie mobile, ces traces sont volontairement générées et conservées pour une durée indéterminée par l'institution bancaire afin de rencontrer diverses exigences commerciales. En effet, *« les banques ont l'obligation de conserver toutes traces de l'ensemble des transactions, tout comme les opérateurs de téléphonie mobile le font. Il y a un devoir de transparence du fournisseur de service vis-à-vis de son client qui doit pouvoir à chaque instant consulter l'historique de ses activités économiques »*²⁴⁶. De la sorte, les établissements financiers s'approprient une véritable possession sur les informations émises par les individus, notamment en ce qui concerne leurs comportements économiques.

Assurément, la carte bancaire constitue, au sein de ce système, un réel outil de traçage électronique à l'instar du téléphone portable. En effet, la collecte des données issues de l'utilisation d'une telle carte permet notamment de « reconstituer les déplacements, les habitudes et les lieux de consommation, la vie personnelle du porteur à savoir ses voyages, ses locations, ses abonnements et ses achats »²⁴⁷. Plus encore que les outils de communication largement utilisés dans la société moderne dont nous avons appris à nous méfier, comme le téléphone portable, une telle carte fournit à notre insu des informations capitales sur nos comportements et nos déplacements.

Se pose dès lors la question de l'usage par les acteurs judiciaires de notre zone territoriale de recherche d'un tel instrument de traçabilité. Quelle est la méthode mobilisée dans ce cadre par la police ? Pour répondre à cette interrogation, nous abordons dans un premier temps la « recherche bancaire ». Sa présentation au sein de notre étude est nécessaire ; cette dernière n'est autre que le moyen d'enquête mis en œuvre par les acteurs judiciaires pour tracer un individu à partir de sa carte de banque. Dans un second temps, nous présentons brièvement, dans le but d'enrichir nos propos, le champ d'application – propre à ce moyen d'enquête en matière de traçabilité – dans lequel celui-ci est mis en œuvre.

²⁴⁶ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁴⁷ M. GAILLARD, « Nouvelles technologies de l'information et de la communication et protection des libertés du citoyen », In *Les libertés individuelles à l'épreuve des NTIC*, sous la dir. de Marie-Christine Piatti, Lyon, Presses universitaires de Lyon, 2001, p. 41.

4.1.2.1. La recherche bancaire

La recherche bancaire désigne la possibilité pour le juge d'instruction de recourir au concours des établissements financiers afin d'obtenir certaines données indispensables à l'enquête pénale. Une telle démarche est légalement instaurée dans le droit belge à l'article 46quater du Code d'instruction criminelle. Il y est indiqué qu'en recherchant les crimes et les délits, le juge d'instruction peut « requérir, s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde, les renseignements suivants :

- a) la liste des comptes bancaires, des coffres bancaires ou des instruments financiers tels que définis à l'article 2, 1^o, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, dont le suspect est le titulaire, le mandataire ou le véritable bénéficiaire et, le cas échéant, toutes les données à ce sujet;
- b) les transactions bancaires qui ont été réalisées pendant une période déterminée sur un ou plusieurs de ces comptes bancaires ou instruments financiers, y inclus les renseignements concernant tout compte émetteur ou récepteur;
- c) les données concernant les titulaires ou mandataires qui, pendant une période déterminée, ont ou avaient accès à ces comptes bancaires »²⁴⁸.

Si la localisation d'une personne par l'usage de sa carte de banque n'est pas expressément mentionnée dans le texte de loi, il n'en demeure pas moins que ce dernier est interprété largement par les professionnels de la justice. De la sorte, parmi les « renseignements concernant tout compte émetteur ou récepteur », figurent notamment les données liées à la détermination géographique d'une transaction économique. Notons que cette localisation n'est toutefois qu'une des multiples facettes offertes par cet article légal.

Selon des considérations générales, « *la recherche bancaire permet de savoir où un individu a effectué un achat ou retiré une somme d'argent et donc de tracer géographiquement le trajet d'une carte, son utilisation et le déplacement de la personne* »²⁴⁹. Verena Reul, juge d'instruction à Eupen nous résume, dans le cadre d'un entretien effectué lors de nos recherches, la motivation de cette « géolocalisation par carte bancaire » rencontrée auprès de l'ensemble des juges interrogés : « *c'est intéressant d'y recourir car cela permet de voir à*

²⁴⁸ Art. 46quater, § 1 du Code d'instruction criminelle.

²⁴⁹ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

*quels endroits ils ont utilisé une carte spécifique. Pour ce faire, nous percevons toute une série de transactions financières. On procède de cette manière lorsque les besoins de l'enquête le justifient pour déterminer, confirmer ou infirmer une localisation »*²⁵⁰. Autrement dit, c'est par le truchement de multiples données conservées par les établissements financiers, comme nous l'avons explicité ci-dessus, et mises par eux à disposition de la justice pénale selon ses besoins qu'une telle géolocalisation est rendue possible. Chaque utilisation d'une carte bancaire est enregistrée et permet en conséquence de fournir des informations capitales sur un vaste nombre d'utilisateurs, pour autant que ces derniers sont suspectés par les autorités judiciaires d'avoir commis un fait pouvant donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou plus²⁵¹.

4.1.2.2. Le champ d'application de la recherche bancaire

La recherche bancaire offre ainsi de précieux renseignements aux acteurs judiciaires. Pour autant, une interrogation demeure : dans quelles situations les acteurs judiciaires mobilisent-ils une telle méthode d'enquête en tant qu'instrument de traçabilité ? Dans la suite cette étude, nous approfondissons cette géolocalisation par carte bancaire en l'illustrant par deux champs d'application dans lesquels celle-ci intervient. Notons que nous insistons sur le fait que ces lignes doivent être lues concomitamment à celles, plus générales, sur l'application de l'ensemble des technologies de traçabilité étudiées dans notre mémoire²⁵².

Tout d'abord, ce moyen d'enquête est mis en œuvre par les autorités judiciaires lorsque ces dernières disposent d'indices sérieux selon lesquels la personne recherchée pour une infraction entraînant une peine d'emprisonnement correctionnelle d'un an ou plus fait un usage fréquent de cartes bancaires. Ce champ d'application est général. Nous pouvons illustrer ce principe avec les propos tenus par Christine Dierick :

« Dans le cadre de mon dossier, un individu suspect avait tué deux personnes. On a fait des devoirs d'enquête pour savoir s'ils avaient utilisé ses cartes après vérification auprès d'une banque. Cela nous a permis de savoir exactement où se trouvait cette personne car celle-ci les avait utilisées à la mer et à Tournai

²⁵⁰ Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

²⁵¹ Voy. Art. 46quater, § 1 du Code d'instruction criminelle.

²⁵² Voy. Section 4.2. Page 85.

*tout en faisant des versements sur un compte particulier. Toutes ces opérations laissent des traces utilisables par la police. Cela permet de localiser les individus et de les identifier lorsque dans mon dossier ils sont introuvables »*²⁵³.

Cette géolocalisation particulière peut, ensuite, être mobilisée dans un cas plus spécifique que le précédent : lors d'un vol de cartes. *« En cas de vol de cartes bancaires, on peut voir, grâce à la recherche bancaire, à quels endroits des retraits ont été effectués ou s'il y a des achats avec cette carte volée. Si celle-ci est utilisée dans un terminal, il y a l'historique qui peut déterminer que l'auteur a utilisé la carte dans un self-banking, ceci étant nécessaire pour orienter les recherches »*²⁵⁴. Luc Golvers, expert judiciaire auprès des services de police, nous confirme cette application particulière dans un entretien que *« lorsque quelqu'un se fait agresser dans une banque et se fait voler sa carte, la police va pouvoir essayer de tracer, avec le système de paiement, l'individu s'il utilise cette carte »*²⁵⁵.

Le champ d'application de la traçabilité par carte bancaire est *in fine* relativement large. À l'intérieur même de ce champ, la masse d'informations recueillies et analysées dans le cadre notamment de la localisation d'un individu est en relation directe avec l'utilisation de cet instrument. Nous pouvons dès lors poser que l'effectivité d'une telle traçabilité mise en place par les acteurs judiciaires dépend, à l'instar de la géolocalisation téléphonique, des utilisateurs eux-mêmes. De tels instruments, fût-ce par leur nécessité ou leur simplicité dans les transactions quotidiennes, occupent aujourd'hui la quasi-totalité de la vie économique du consommateur moderne et dont les activités, en conséquence, modèlent indéniablement les pratiques policières de surveillance.

4.1.3. La base de données commerciales

Parler de traçabilité implique que soient réunis plusieurs éléments : il faut qu'il y ait des traces numériques et donc un support qui puisse les créer ; il convient ensuite d'avoir un mécanisme légal pour autoriser le recueil de ces traces ; et enfin il est nécessaire de disposer d'une structure informatique qui permette de les traiter et de les analyser pour en tirer d'adéquates

²⁵³ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁵⁴ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁵⁵ Entretien avec Monsieur Luc Golvers réalisé le 17 mars 2016.

conclusions²⁵⁶. Assurément, le téléphone portable et la carte de banque constituent un support matériel de traçabilité. Par leur usage, une série de traces se sont répandues dans un environnement diffus et immatériel, et dont certains mécanismes juridiques en imposent le recueil et la rétention comme nous avons pu le constater²⁵⁷. De telles informations sont subséquemment conservées au sein d'une structure particulière : la base de données. Ce dernier instrument de traçabilité constitue l'objet d'étude de cette section. Une telle base de données pourrait être globalement définie comme « une masse d'informations sous forme de codes numériques, stockées sur des disques durs fermés ou sur des serveurs connectés et classifiées selon des catégories tout en offrant des modalités d'accès structurées »²⁵⁸. Certes, la localisation d'un individu particulier n'est pas l'objectif premier de ces regroupements informationnels. Toutefois, sous le prisme de la traçabilité, ces instruments permettent d'archiver, d'analyser et de reconstituer des comportements et déplacements ayant au préalable disséminé une trace numérique.

Notons que les premiers traits de cette structure informatique ont préalablement été esquissés pour constater son importance dans l'application des mécanismes de partage et de tri social au sein de la société de surveillance. Nous renvoyons le lecteur aux points 3.1. et 3.3. pour un rappel d'informations élémentaires. L'objectif de cette section vise toutefois à présenter un aspect non plus général mais particulier des bases de données détenues par des entreprises commerciales : le transfert de données vers les services de police et les juges d'instruction des arrondissements judiciaires en Wallonie. Les services de police ont-ils recours aux entreprises commerciales et à leurs bases de données pour apprécier les déplacements d'un individu suspect ? Autrement dit, existe-t-il dans le cadre de la traçabilité des personnes un véritable transfert de données commerciales vers les autorités judiciaires ? Pour ce faire, nous devons effectuer une distinction parmi les entreprises, entre celles dont le concours est rendu obligatoire par des textes légaux et celles dont la collaboration ne l'est pas en l'absence de telles normes.

La première catégorie d'entreprises regroupe principalement les opérateurs de téléphonie mobile et les institutions bancaires. Comme nous l'avons abordé en plusieurs points, la Belgique s'est pourvue de mécanismes légaux facilitant l'accès et le partage de données. Ces

²⁵⁶ M.-A. HERMITTE, « La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise », In *Traçabilité et responsabilité*, sous la dir. de Philippe Pédrot, Paris, Economica, 2003, p. 41.

²⁵⁷ Voy. Point 3.1.2.3. p. 53.

²⁵⁸ É. SADIN, *op. cit.*, p. 114.

entreprises sont ainsi dans l'obligation de fournir certaines informations, recueillies préalablement dans leurs bases de données, pour permettre la géolocalisation d'un individu. « *On se sert beaucoup de Proximus et d'autres fournisseurs comme Base et Mobistar au même titre que les banques. On les y oblige* »²⁵⁹. La collaboration entre ces différents acteurs et le transfert de données en fonction des besoins de l'enquête pénale apparaissent ainsi être extrêmement fréquente.

La seconde catégorie est quantitativement beaucoup plus importante. Celle-ci regroupe l'ensemble des entreprises dont la coopération avec les autorités judiciaires n'a pas été rendue obligatoire. Le principe général est le suivant : « *Tout ce qui existe dans le monde réel et virtuel, tout ce qui est accessible à un moment donné, si la procédure le permet et que l'on dispose des justifications par rapport à l'implication d'une personne, peut être sollicité* »²⁶⁰. Pour autant, les sollicitations de la justice auprès de ces entreprises demeurent soumises au bon vouloir de celles-ci, de telle sorte que « *certaines entreprises ne donnent pas suite aux demandes insistantes du juge* »²⁶¹. A l'aune des réponses apportées par les personnes interrogées dans le cadre de nos recherches, il semblerait que la contribution de grandes entreprises commerciales de cette catégorie comme Google, Apple, Facebook, Amazon ou Microsoft soit peu fréquente. Ainsi, comme l'affirme Martine Michel, « *non, je n'ai pas encore ressenti l'utilité d'y recourir mais c'est quelque chose qui pourrait dans un avenir proche être important* »²⁶².

Le recours aux entreprises commerciales par les autorités judiciaires et les services de police dans le cadre de la traçabilité est par conséquent avéré, quoique ce principe nécessite d'être nuancé. Un transfert de données existe entre les différents acteurs susmentionnés dont la fréquence dépend de la société en tant que telle. Ce phénomène dont nous avons souhaité esquisser les traits dans un contexte délimité, celui de l'enquête pénale, dépasse cependant largement un tel contour et pose la question essentielle de l'intégrité de la personne et de son droit à la vie privée, question à laquelle nous laissons le lecteur libre d'y répondre : pouvons-nous accepter que nos données personnelles soient partagées à notre insu ?

²⁵⁹ Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

²⁶⁰ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

²⁶¹ Entretien avec Monsieur Luc Golvers réalisé le 17 mars 2016.

²⁶² Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

4.2. L'usage des technologies numériques de traçabilité dans l'enquête pénale

La recherche de preuves matérielles a de tout temps constitué l'essence des enquêtes pénales menées par les différents acteurs judiciaires. Il importe de pouvoir déterminer, par la constitution d'éléments probants, l'établissement de la réalité d'un fait afin d'aboutir notamment à la manifestation de la vérité. A cet égard, les technologies numériques de traçabilité étudiées préalablement jouent un rôle considérable. Comme nous l'explique Christine Dierick, le recours au traçage des individus va permettre aux différents acteurs judiciaires de déterminer toute une série d'éléments fondamentaux : *« après une infraction particulière, la traçabilité d'un individu permet d'établir la période infractionnel, l'identification de l'auteur et de l'ensemble des personnes en lien avec celui-ci et l'endroit où le fait a été commis. Ce sont trois éléments essentiels permettant de qualifier l'infraction et d'en inculper les individus »*²⁶³.

L'usage des technologies de traçabilité numérique revêt ainsi une certaine importance au sein de l'enquête pénale eu égard aux éléments susmentionnés qu'il établit. Plus précisément, de tels éléments de preuve rassemblés par la géolocalisation *« offre une bonne appréciation des faits infractionnels. Si un individu affirme qu'il était à un tel endroit et à tel moment alors que les différents moyens techniques prouvent le contraire... Cette traçabilité va nous donner les informations qui vont pouvoir l'écarter ou non de l'enquête »*²⁶⁴. Autrement dit, la traçabilité présente *« l'avantage de permettre de récupérer toute une série d'indices incontestables que les devoirs d'enquête classiques ne nous permettraient pas »*²⁶⁵.

En conséquence, ces instruments que nous avons abordés individuellement pour en comprendre les mécanismes sont devenus *« presque incontournables pour le juge d'instruction »*²⁶⁶. Pour autant, leur mobilisation n'est pas automatique ! Quand est-il possible pour un magistrat instructeur de mettre en œuvre une mesure de traçabilité ? Pour aborder cette interrogation, nous estimons opportun de présenter, en termes généraux, les modalités d'application de ces moyens d'enquête. D'une part, l'usage des technologies numériques de traçabilité est soumis à des critères cumulatifs que le juge d'instruction doit nécessairement apprécier dans la direction de son enquête. L'énumération et l'analyse de tels critères

²⁶³ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁶⁴ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁶⁵ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁶⁶ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

constituent la première section de ce chapitre. D'autre part, cette utilisation est adaptée à l'affaire que doit résoudre le juge. Nous imaginons mal le recours aux instruments de traçabilité dans le cadre de violences intrafamiliales. Le champ d'application de ces instruments forme par conséquent la deuxième section de ce chapitre.

4.2.1. Les critères d'application

L'usage d'une technologie de traçabilité numérique par les autorités judiciaires est, d'une manière générale, tributaire de critères informels dont les contours et limites restent, dans une large mesure, nébuleux. Afin de pouvoir mettre en place ce type d'instrument, le juge d'instruction apprécie nécessairement une série de données propres au dossier dans le cadre duquel une intervention de cet ordre est envisageable. Ce n'est qu'après avoir rencontré la satisfaction des « critères de traçabilité » qu'une telle mise en place est possible. Issus de la pratique, ceux-ci ne répondent toutefois à aucun prescrit légal ni à aucune norme formulée en cette matière ; ils sont en effet soumis à l'appréciation souveraine, personnelle et subjective, du magistrat instructeur. *« Les critères d'application d'une technologie numérique de traçabilité sont clairement sujets à la libre évaluation du juge »*²⁶⁷.

Au demeurant, quels sont ces différents critères d'application d'une technologie numérique de traçabilité ? S'ils ne répondent à aucune norme juridique prédéfinie dans un texte légal, la conduite d'entretiens dans le cadre de notre recherche a permis de déboucher sur des critères communément employés par les juges d'instruction interrogés. Ces derniers, que nous analysons dans les développements subséquents, sont au nombre de quatre : l'opportunité et la valeur ajoutée – le coût de la mesure – la faisabilité technique – et le respect des normes juridiques en matière de vie privée.

4.2.1.1. L'opportunité et la valeur ajoutée

Le premier critère que doit rencontrer tout juge d'instruction souhaitant mobiliser un instrument de traçabilité numérique est l'opportunité et la valeur ajoutée de ce moyen technique dans l'enquête pénale. Cet instrument offre-t-il l'opportunité d'obtenir des informations d'une certaine valeur ? Il s'agit d'un véritable critère tactique débattu entre les

²⁶⁷ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

différents acteurs judiciaires. Ainsi, la traçabilité d'un individu « *n'est pas automatiquement activée par la police dans tout type de dossier car il n'y a peut-être pas l'opportunité de le faire et la valeur ajoutée des éléments obtenus sera nulle* »²⁶⁸. Verena Reul estime dans cette optique que « *lorsqu'il est notamment opportun de localiser un individu à partir de son numéro de gsm, nous procédons à sa géolocalisation* »²⁶⁹. En définitive, il revient au « *magistrat instructeur de déterminer si ce moyen mis en œuvre présente une réelle opportunité et une valeur ajoutée* »²⁷⁰.

4.2.1.2. Le coût de la mesure

Le coût de la mesure constitue le second critère d'application d'une technologie numérique de traçabilité. Tout moyen d'enquête doit financièrement être abordable pour être mis en œuvre par un juge d'instruction. Or, le recours aux nouvelles technologies en ce compris celles relatives à la traçabilité implique des frais financiers importants. Il est donc fondamental, pour des raisons d'ordre budgétaire, d'apprécier minutieusement le coût de la mesure sollicitée dans le cadre d'une enquête pénale. Jean-François Joris nous résume parfaitement un tel principe :

*« Il y a aussi un critère au niveau du coût, qui s'ajoute à l'opportunité et la plus-value, pour déterminer la mise en place d'un instrument de traçabilité. Il y a certaines choses qui parfois pourraient être réalisables mais qui seraient disproportionnées en matière d'engagement ou de frais de justice. Il y a en conséquence une véritable évaluation financière à réaliser par rapport à une mesure de traçage que l'on souhaite mettre en place »*²⁷¹.

4.2.1.3. La faisabilité technique

Mobiliser un instrument de traçabilité numérique implique, pour la justice pénale, la disponibilité d'un certain savoir-faire technique. Si un moyen d'enquête permettant de tracer un individu dans le cadre d'investigations policières présente une réelle opportunité de procurer des informations précieuses, encore faut-il que celui-ci soit, sans mentionner le coût

²⁶⁸ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

²⁶⁹ Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

²⁷⁰ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁷¹ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

de la mesure, faisable techniquement. Tel est le troisième critère devant être apprécié lors du recours aux technologies de traçabilité. A cet égard, Christine Dierick affirme sans détour le postulat suivant :

« Il y a également une évaluation sur la faisabilité technique. Beaucoup de choses sont faisables en matière de traçabilité mais il faut voir si dans le cas d'espèce, on a les moyens, si c'est réalisable techniquement pour nous. Ce n'est pas parce qu'on souhaite le faire qu'on peut le faire dans un dossier bien déterminé. Il y a toute une évaluation qui est faite en bonne intelligence entre police et magistrats. Le mot final est toujours dans le chef du magistrat »²⁷².

Une infaisabilité technique est ainsi, en tant que critère d'application d'une technologie de traçabilité, susceptible d'empêcher le recours à de tels instruments. Celle-ci peut aisément être illustré par les propos tenus par Martine Michelle : *« Nous suivons difficilement l'évolution des technologies numériques de la société. Ce n'est pas véritablement notre matière, c'est très compliqué ; il nous faut des experts techniques »²⁷³*. Assurément, le pouvoir judiciaire est toujours à la poursuite des évolutions technologiques de la société civile, qui évolue au gré et aux humeurs des individualités les plus créatives. Pris en créneau entre une société qui évolue à vitesse grand V, d'autant plus au niveau de la technologie, et des contraintes budgétaires toujours plus importantes, les autorités judiciaires et les services de police rencontrent de véritables contraintes techniques dans la mobilisation de nouveaux moyens d'enquête pouvant apporter une réelle plus-value à l'enquête pénale. Les technologies de traçabilité numérique n'échappent guère à cette tendance.

4.2.1.4. Le respect des normes juridiques en matière de vie privée

Le dernier critère d'application d'une technologie numérique de traçabilité se rapporte au respect des garanties légales protégeant notre vie privée. De telles garanties, instituées de manière éparse dans différents textes juridiques et non spécialement dans le cadre de la traçabilité, sont essentielles : en Belgique, toute personne a droit au respect de sa vie privée et familiale. Cette protection est d'autant plus importante que les instruments de traçabilité revêtent un caractère intrusif eu égard aux données qu'ils collectent. *« Tout ce qui est intrusif*

²⁷² Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁷³ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

*au niveau de la vie privée est terriblement réglementé et c'est normal. On ne fait pas ce que l'on veut, comme on veut, quand et n'importe comment ! C'est un aspect que la police doit prendre en compte »*²⁷⁴.

Dès lors, la protection légale de la vie privée constitue assurément pour les acteurs judiciaires un véritable critère d'application d'une mesure de traçabilité. *« C'est toujours intéressant au niveau des informations perçues de recourir à ces technologies mais il faut mettre en balance un tel recours avec le respect de la vie privée »*²⁷⁵. Par conséquent, ce dernier critère influence véritablement l'application d'une mesure de traçabilité dans une enquête pénale. Jean-François Joris nous démontre ce postulat : *« ce n'est pas parce qu'on peut d'emblée faire ceci ou cela au niveau technique que légalement il est opportun de le faire. On choisit en bon père de famille, en respect de toutes les normes légales par la justification dans le réquisitoire des moyens les plus intrusifs »*²⁷⁶.

4.2.2. Le champ d'application

Tributaire de plusieurs critères cumulatifs et officieux, l'application d'une mesure de traçabilité numérique n'est guère actée librement. La mise en œuvre de ces mesures intrusives est soumise, eu égard aux enseignements de la section précédente, à des garde-fous restrictifs dans l'exercice des pouvoirs judiciaires par les différents acteurs intervenant au sein d'une enquête pénale. Certes, l'ensemble de ces critères doit être conjugué par le juge d'instruction pour procéder à l'usage d'une technologie numérique de traçabilité. Toutefois, encore faut-il pouvoir employer ces instruments dans un champ d'application adéquat ! En effet, cette mobilisation est nécessairement adaptée à l'affaire que doit résoudre le juge. Tel est l'objet d'étude de cette section dont le principe général est le suivant : *« l'importance de la traçabilité dépend aussi d'un dossier et de ses caractéristiques. Un dossier n'est pas l'autre. Ce genre d'outils peut être utile dans une affaire particulière mais ne le sera pas dans une autre. Cela dépend vraiment des contingences, des possibilités et des éléments dont on dispose »*²⁷⁷.

²⁷⁴ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁷⁵ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

²⁷⁶ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

²⁷⁷ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

Les propos de Stéphane Kerkhofs sont ainsi parfaitement illustratifs du champ d'application et de son principe général : c'est en fonction du dossier et de ses caractéristiques inhérentes qu'un juge d'instruction a recours aux instruments de traçabilité. Dès lors, dans quelles affaires pénales les acteurs judiciaires mobilisent-ils ces moyens techniques ? Nous avons souhaité, dans le cadre non-exhaustif de ces développements, mettre l'accent sur les principaux dossiers dans lesquels une mesure de traçabilité numérique est susceptible d'être employée.

Christine Dierick nous expose une première illustration du champ d'application : « *il y a des dossiers où l'on sait par la nature des faits du dossier qu'il y aura sûrement de la traçabilité. Par exemple, dans un dossier de stupéfiants, il y a généralement de la téléphonie. En l'occurrence, un tel dossier sans téléphonie est assez rare* »²⁷⁸. La lutte contre les stupéfiants constitue ainsi une première sphère d'action majeure au sein de laquelle une mesure de traçabilité est susceptible d'être appliquée. Une telle application s'explique aisément, selon les dires de Martine Michelle, en fonction des spécificités des infractions liées aux stupéfiants : « *Dans un tel dossier, j'ai souvent besoin de savoir où la personne va se servir et se ravitailler, où elle stocke et qui elle va voir comme potentiels clients. Cela sera forcément intéressant de pouvoir, dans ce cadre, tracer l'individu pour déterminer les chemins qu'elle a empruntés* »²⁷⁹.

Les dossiers d'homicide constituent une seconde illustration du champ d'application de la traçabilité numérique. « *Pour prendre l'exemple d'un dossier d'homicide, il est très intéressant de connaître, grâce à la géolocalisation, l'emploi du temps d'un individu avant, pendant et juste après la commission des faits* »²⁸⁰. Dans cette optique, les données de localisation en considération de cette période infractionnelle constituent le ressort principal du recours à la traçabilité d'une personne. Ce dernier est ainsi inscrit dans une deuxième sphère d'action ; celle relative aux affaires d'homicide. Comme l'affirme Martine Michelle : « *dans ce genre de dossiers, pour savoir si l'auteur est passé par là, nous pouvons le déterminer par le fait qu'il ait notamment actionné son GSM dans un tel endroit. Nous pouvons repérer par la traçabilité le passage de la personne qui fut à proximité des lieux du crime* »²⁸¹.

²⁷⁸ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁷⁹ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

²⁸⁰ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁸¹ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

Le dernier champ majeur d'application d'une mesure de traçabilité se rencontre dans le cadre des associations de malfaiteurs et des organisations criminelles. « *Une association de malfaiteurs dont l'existence est légalement incriminée dans un article du code pénal commet généralement des infractions dont la nature peut être propice au traçage* »²⁸². Cette dernière sphère d'action, favorable à cette mesure, repose grandement sur le flux des communications électroniques échangées entre les différents acteurs du groupement criminel. Stéphane Kerkhofs résume explicitement, dans ce cadre particulier, l'essence de la traçabilité :

*« Dans des dossiers où il y a la notion d'organisation criminelle, la traçabilité notamment téléphonique va être déterminante pour pouvoir déterminer la chaîne de communication entre les différents intervenants et par là aussi le rôle de chacun dans l'organisation. Il est ainsi souvent nécessaire de procéder à la localisation des individus dans les dossiers d'organisation criminelle en matière de stupéfiants ou même dans les matières de trafic de toute sorte d'armes, de véhicules, etc. »*²⁸³.

En définitive, le champ d'application d'une technologie numérique de traçabilité est relativement large ; nous l'avons illustré par trois physionomies récurrentes auprès des juges d'instruction interrogés. Toutefois, nous insistons pleinement sur le fait qu'un tel champ n'est en aucun cas limité à ces exemples. Les autorités judiciaires peuvent *in fine* recourir à la traçabilité d'une personne dans le cadre, par exemple, d'une affaire de vol avec violence pour autant que le dossier et ses caractéristiques inhérentes – comme l'usage d'une carte bancaire ou d'un téléphone portable – le permettent.

4.3. La synergie des technologies numériques de traçabilité

Contrôlée et délimitée, l'application d'une technologie de traçabilité numérique par les juges d'instruction et les services de police dans les arrondissements judiciaires en Wallonie s'inscrit dans une recherche mesurée d'éléments probatoires. La détermination des déplacements et de la localisation d'un individu sur lequel repose les soupçons de la justice, par un instrument de traçage numérique, est, à cet égard, fondamentale. Pour autant, il serait illusoire de croire en leur mobilisation unique et exclusive de toute autre technologie et

²⁸² Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁸³ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

moyen d'enquête. Les pratiques des différents acteurs interrogés témoignent *a contrario* d'une synergie des méthodes de traçabilité avec d'autres techniques particulières d'enquête.

« Alors que les capacités de technologies considérées individuellement sont importantes, il est fondamental de souligner la croissance de la convergence de différentes technologies et autres méthodes policières »²⁸⁴. Tel est l'essence de la synergie, étudiée dans cette dernière partie relative aux nouvelles technologies, pleinement répandue dans les enquêtes pénales. Dans ce cadre, la traçabilité et ses supports matériels s'inscrivent assurément dans cette convergence des moyens d'enquête. « *Une personne ne sera pas condamnée simplement sur la base d'un historique de téléphonie mobile* »²⁸⁵. Ce principe repose sur une motivation singulière ; celle d'accroître l'efficacité, en termes de recherche et de collecte de données, des méthodes mises en œuvre. Ainsi, de multiples techniques de récolte d'informations jointes ensemble sont beaucoup plus efficaces que la somme individuelle de chacune d'entre elles²⁸⁶.

Concrètement, l'ensemble des juges d'instruction interrogés dans le cadre de nos recherches confirme implicitement la synergie des technologies de traçabilité numérique. Comme l'affirme Stéphane Kerkhofs, « *il n'y a pas une traçabilité seule qui va servir à déterminer les déplacements d'un auteur ou à le faire condamner. C'est un éventail d'indices et d'éléments de nature tout à fait différente qui vont être mis bout à bout par des méthodes convergentes pour conclure une enquête. La traçabilité n'est jamais qu'un outil parmi d'autres* »²⁸⁷. Verena Reul illustre, quant à elle, parfaitement l'incidence de la synergie attachée aux instruments de traçabilité sur les pratiques des acteurs judiciaires :

*« Il faut soutenir ces éléments de traçabilité par d'autres éléments. Il faut coupler la géolocalisation par une convergence d'autres moyens, preuves, éléments comme une écoute téléphonique. C'est un outil parmi d'autres pour obtenir un faisceau de présomption. Dans mon dossier, j'indique qu'un tel individu a été borné à tel endroit, que des caméras de reconnaissance automatique des plaques ont flashé une plaque particulière, tout en corroborant mes éléments avec le témoignage d'un individu »*²⁸⁸.

²⁸⁴ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 26.

²⁸⁵ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

²⁸⁶ J. STANLEY & B. STEINHARDT, *op. cit.*, p. 11.

²⁸⁷ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

²⁸⁸ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

Cette synergie reconnue par les différents acteurs judiciaires permet finalement, à l'aune de ces extraits, de relativiser l'emploi de la traçabilité dans une enquête pénale. Certes, un tel usage est susceptible d'être essentiel dans la collecte de certaines données. Nous avons pu l'aborder longuement au sein de ce chapitre. Celle-ci n'est, cependant, qu'une méthode parmi l'arsenal considérable de moyens d'enquête mis à la disposition des magistrats instructeurs par lesquels ils la suppléent. Une nécessaire relativité est, par conséquent, de mise.

5. Conclusion

La surveillance, entendue comme une attention soutenue à nos données personnelles au sein d'une société dont l'organisation et la structure repose sur une assise technique, n'est donc pas une pure création de l'esprit, un concept abscons et sans fondement : nous voyons qu'elle se décline matériellement à travers différents mécanismes dont il est possible d'en apprécier la teneur. À la base se situe le partage de l'information, de manière volontaire ou non, consciemment ou non, par les utilisateurs de toute une série d'appareils et de technologies qui laissent des traces plus ou moins difficilement exploitables. C'est l'exploitation même de ces traces, par un détournement d'usage, qui constitue la surveillance. Téléphone portable, carte bancaire... la liste est longue. Se déroulent ensuite différentes opérations intellectuelles destinées à exploiter la quantité importante de ces informations dans une visée et vers des buts spécifiques : contrôler, réguler, gérer ou influencer un groupe d'individus. Dans la poursuite de ses objectifs, ces mécanisme-clés constituent à l'heure actuelle le cœur du fonctionnement de la société de surveillance.

De tels mécanismes reposent nécessairement sur une assise technologique : pour les mettre en œuvre, la surveillance doit notamment mobiliser certaines technologies de traçabilité numérique, instruments sur lesquels les autorités judiciaires lorgnent avec une certaine avidité. Il est, de la sorte, fréquent que les autorités judiciaires et les services de police les utilisent selon des critères d'application particuliers dans un champ d'application spécifique. Autrement dit, la traçabilité intervient au service de ces acteurs dans une enquête pénale, tout en étant produite par l'ensemble des citoyens qui utilisent ces technologies susceptibles de laisser des traces. Lesdites technologies ayant envahi le quotidien dans notre société moderne, le volume de traces et d'informations à la disposition des autorités étatiques peut laisser perplexe quant à leur exploitation diverse et variée dans une enquête pénale.

Pour autant, la société de surveillance telle que nous l'avons décrite est-elle une réalité tangible au sein des pratiques employées par les autorités judiciaires et services de police dans les limites territoriales de notre étude lors d'une enquête pénale sous le prisme de la traçabilité de tout un chacun ?

Quatrième partie :
Sommes-nous dans une Société de Surveillance ?

1. Introduction

« Nous finirons peut-être par moins redouter un État surveillant
qu'un État incapable de savoir qui surveille qui »

- François-Bernard Huyghe ; *Téléphonie mobile : capter la vie numérique des autres* (2009)

De nombreuses interrogations ont esquissé l'ébauche de notre étude. Devons-nous craindre une surveillance omniprésente ? Nous dirigeons-nous vers la société de surveillance totale décrite par Georges Orwell dans son célèbre roman *1984* ? À quelles conditions pouvons-nous faire confiance aux structures étatiques d'en user à bon escient ? Quels sont les tenants et aboutissants d'une surveillance indiscriminée menée par les acteurs judiciaires en Belgique ?

Au regard de ces interrogations, la société de surveillance et ses diverses manifestations concrètes constituent le centre névralgique de notre étude. Mû par la volonté de comprendre et de démontrer son éventuelle existence à l'échelon local, nous avons analysé les principaux traits – tels que la définition, les mécanismes et les technologies – de cette société grâce à diverses contributions littéraires et orales. Suite à ces considérations, il nous paraît à présent opportun d'aborder la question centrale de ce mémoire : pouvons-nous conclure à l'avènement, au sein de notre zone territoriale, d'une telle société eu égard à l'usage d'instruments de traçabilité numérique par les autorités judiciaires et les services de police ?

À ce sujet, nous estimons ne pas être dans une société de surveillance généralisée. « *Big Brother, certainement pas. Il faut relire le livre 1984 pour se rendre compte que l'on est avant tout dans un système où tout le monde n'est pas surveillé...* »²⁸⁹. Certes, la traçabilité numérique des individus procure aux acteurs judiciaires une réelle opportunité de surveillance. Toutefois, « *si on est tous traçables, cela ne veut pas dire qu'on est forcément tous surveillés. Est-ce que l'on vit dans une société au sein de laquelle nous sommes tous surveillés ? Je suis nuancé par rapport à ça. On est certes tous traçables, mais être traçable ne veut pas dire être surveillé. Être surveillable ne veut pas dire être surveillé* »²⁹⁰. La société de surveillance ne semble pas ainsi être une réalité actée au sein des pratiques judiciaires. Comment l'expliquer ? Nous considérons, après une recherche minutieuse, qu'une série d'obstacles s'érige à l'encontre de celle-ci. Sur base d'articles scientifiques et d'entretiens effectués auprès de certains acteurs judiciaires, nous abordons, dans la suite des développements, ces obstacles empêchant l'avènement d'une telle surveillance généralisée.

²⁸⁹ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²⁹⁰ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

2. Les obstacles à l'établissement d'une Société de Surveillance

Dans le champ restreint de la traçabilité numérique, le recours à ces technologies par les autorités judiciaires et les services de police n'instaure pas en Wallonie une société de surveillance généralisée. Ce cadre susmentionné est fondamental ; l'ensemble des pratiques de surveillance ne se limite pas aux acteurs judiciaires ayant recours au suivi des individus. D'autres contextes – étatiques ou commerciaux, aux États-Unis ou au Royaume-Uni – sont susceptibles d'être favorables à l'établissement d'une surveillance généralisée. Tel n'est toutefois pas le cas dans l'exercice de la traçabilité par les acteurs que nous avons interrogés.

En effet, un tel exercice n'est pas libre de toute contrainte. D'une part, nous avons pu observer l'obligation pour le juge d'instruction de prendre en considération certains critères propres à l'application des mesures de traçabilité. S'ils ne constituent pas en tant que tels de véritables barrières, dans le sens où leur objectif premier est de permettre la mise en œuvre adéquate de ces devoirs d'enquête, il n'en demeure pas moins que ces critères empêchent un recours démesuré aux technologies numériques de traçabilité. D'autre part, nous avons également pu constater, auprès des différents acteurs interrogés, l'existence d'obstacles dans l'application de différentes mesures de surveillance par les autorités judiciaires. S'ils dépassent largement le cadre de la traçabilité au vu de leur caractère éclectique, ceux-ci s'y intègrent et en restreignent, par une répercussion commune, considérablement l'usage.

Plus précisément, ces obstacles à l'établissement d'une société de surveillance axée sur la traçabilité concernent le manque de personnel pour gérer une quantité toujours plus importante de données – le manque de moyens financiers – de nombreuses contraintes juridiques – et l'adaptation des délinquants aux mesures de traçabilité mises en œuvre par les acteurs judiciaires. Dans les sections suivantes, nous analysons l'ensemble de ces obstacles et leur incidence sur la traçabilité en tant que mesure de surveillance.

2.1. Le manque de personnel et la quantité trop importante de données

Le manque de personnel adéquat et compétent est une plainte lancinante émanant des autorités judiciaires et des services de police. Confrontée au problème d'un personnel en sous-effectif, la justice peine à remplir l'ensemble des missions qui lui sont attribuées. Selon

Christine Dierick, *« nous n'avons pas assez d'effectifs, d'analystes. Ils sont toujours débordés et pourtant, leur travail est capital. Il y a certainement un manque de moyens au niveau des services de police. Au niveau des juges d'instruction, on a un énorme retard à cause d'un sous-effectif »*²⁹¹. Jean-François Joris témoigne également de ce problème rencontré au sein de son service de police : *« mon office est complètement débordé et il a fallu attendre six mois pour analyser une pièce à conviction. Ce n'est pas vivable. Donc, l'inconvénient des nouvelles technologies notamment en matière de traçabilité, c'est la charge énorme de travail conjuguée au manque d'effectif »*²⁹². Un tel constat est alarmant car : *« nous arrivons au stade où soit nous ne savons plus travailler, soit nous commettons des erreurs »*²⁹³. Une surveillance de masse organisée par les autorités judiciaires n'est, dans cette optique, pas envisageable ! Plus particulièrement, celles-ci rencontrent de réelles difficultés dans l'application de différentes mesures de surveillance en raison, d'une part, d'un manque évident de personnel adéquat et compétent pour la gestion, d'autre part, de données dont la quantité ne cesse de croître, comme nous le verrons au paragraphe suivant.

En presque une décennie, le nombre de communications via les infrastructures électroniques de la société a explosé. Une pluralité d'échanges communicationnels peut ainsi être observé entre les individus, pluralité sur laquelle se basent nécessairement les acteurs judiciaires pour déterminer avec une précision relative la localisation de ces derniers par le biais de la traçabilité téléphonique ou bancaire. Pour autant, cette exigence de multiplicité des données au sein d'une « logique de masse », dont le caractère intrusif est indéniable, entraîne certaines difficultés. « Si les outils de géolocalisation des appareils techniques de nouvelle génération font redouter à certains une société *Big Brother*, l'accroissement exponentiel du volume des échanges, sous la forme de conversations audio, de SMS, de e-mails, voire même de transactions bancaires, rend la surveillance des menaces très compliquée »²⁹⁴. Une tentative d'accumulation massive de données peut ainsi se révéler, aussi séduisante soit-elle, contre-productive eu égard aux enjeux sécuritaires pour lesquels elle intervient.

Par conséquent, une quantité toujours plus importante de données disséminées après l'usage d'instruments de traçabilité attire les services de police, certes compétents pour les traiter qualitativement mais en sous-effectif, vers une impossibilité opérationnelle de mettre en place

²⁹¹ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁹² Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

²⁹³ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

²⁹⁴ M. TRÉVIDIC, *Au cœur de l'antiterrorisme*, Paris, JC Lattès, 2011, p. 242.

des mesures de surveillance. Au plus un nombre important d'individus abandonnent massivement des traces, au moins la surveillance des autorités judiciaires est effective. Verena Reul résume parfaitement ce premier obstacle à l'établissement d'une société de surveillance dans le cadre de la traçabilité numérique :

« Il y a tellement de communications échangées que cela devient presque inexploitable. C'est en raison de l'explosion des communications que nous avons des difficultés d'exploitation des données. La police doit analyser les données émises mais en raison de son sous-effectif et des quantités de données, cela devient impossible pour nous de tout analyser. La police doit lire toutes les données de communication, comprendre les langues étrangères, etc. On rencontre de véritables difficultés suite à l'explosion des communications. Il y a trop de téléphones portables, de téléphonie pour permettre une surveillance correcte de l'ensemble des GSM qui nous intéressent dans le cadre d'une enquête pénale »²⁹⁵.

2.2. Le manque de moyens financiers

Procéder à la surveillance indiscriminée d'une population implique la mobilisation de moyens financiers colossaux. La récolte, l'enregistrement et l'analyse de nos données personnelles par l'usage de diverses technologies de traçabilité requièrent l'allocation d'un budget conséquent²⁹⁶. « Utiliser ce genre de technologie coûte cher »²⁹⁷. La problématique financière ne peut de la sorte être éludée par les acteurs judiciaires dans le cadre d'une enquête pénale. Ainsi, intervient nécessairement dans les questions sécuritaires et de surveillance un « régulateur économique ». Vincent Francis en explicite le fondement :

« Les pratiques de surveillance, dans une démocratie, à des fins judiciaires, ne s'appliquent pas à l'ensemble de la population pour des motifs purement économiques. Même en matière de sécurité, il y a une logique économique qui prime. (...) On ne va pas surveiller tout le monde si cela ne vaut pas la peine de surveiller tout le monde. Le travail policier implique clairement un travail

²⁹⁵ Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

²⁹⁶ Voy. Point 4.1.1.3. p. 75, en ce qui concerne la téléphonie mobile.

²⁹⁷ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

économique. L'idée, c'est de se focaliser sur une partie la plus petite possible de la population. Nous ne sommes pas au niveau judiciaire dans un contrôle et une surveillance de masse »²⁹⁸.

À l'instar d'une pénurie flagrante de personnel pour la gestion de multiples données, le manque de moyens financiers constitue donc un second obstacle à l'établissement d'une société de surveillance dans le cadre de la traçabilité numérique. Plus précisément, c'est en considération d'un tel manque qu'interviennent, selon les termes de Vincent Francis, des motifs économiques dans la mise en œuvre de mesures de surveillance par les acteurs judiciaires. La gestion en *bon père de famille* des deniers publics incite, en effet, ces derniers à la vigilance dans le choix de pratiques onéreuses. Des impératifs financiers s'immiscent ainsi dans l'application d'instruments technologiques au sein des enjeux sécuritaires de la société actuelle. Notons que ce manque de moyen entraîne, comme nous l'avons abordé dans les chapitres précédents, une participation, encadrée par la loi en Belgique, de certains acteurs privés au cœur des pratiques de surveillance des acteurs étatiques et judiciaires²⁹⁹.

Cette tendance n'est pas prête de s'estomper, bien au contraire ! Si les juges d'instruction ne sont pas contraints à l'heure actuelle par une limite budgétaire – ce qui ne veut pas dire qu'ils puissent dépenser sans compter eu égard aux considérations précédentes – les réformes législatives futures tendent à supprimer cette « liberté financière ». En effet, le gouvernement belge planche présentement sur l'adoption d'une « gestion autonome pour l'organisation judiciaire ». Cette loi vise plus particulièrement à établir un budget limité chaque année pour l'ensemble des juges d'instruction, seuil qu'ils ne pourront dépasser. *« L'autonomie de gestion sur le point d'être votée va mettre encore plus en péril cette possibilité de recourir à des mesures coûteuses de surveillance. Pour l'instant, quand je fais une expertise téléphonique, le ministère paye automatiquement. Là, on va devoir calculer les mesures à réaliser en fonction du budget qui nous sera alloué »*.³⁰⁰ Une mesure de traçabilité numérique devra ainsi être minutieusement appréciée avant sa mise en œuvre, au possible préjudice du recours à d'autres instruments de traçage lors d'enquêtes ultérieures en raison d'un budget réduit à peau de chagrin ! Il apparaît, dès lors, peu probable l'établissement d'une société de surveillance en considération des budgets sans cesse réduits des juges d'instruction.

²⁹⁸ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

²⁹⁹ Voy. Section 2.5. p. 28 & sous-section 3.1.2. p. 50.

³⁰⁰ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

En définitive, Martine Michel synthétise les propos recueillis auprès des juges d'instruction interrogés lors des différents entretiens. Elle souligne implicitement l'importance du « régulateur économique » dans les questions sécuritaires et de surveillance s'inscrivant, pour notre part, à l'encontre d'un tel établissement :

« Dans le futur, on va avoir une gestion autonome de nos enquêtes. On va donc avoir cette espèce de budget prédéfini qui va déterminer notre marge d'action dans nos enquêtes. Cela va nécessairement impacter le recours aux nouvelles technologies de traçabilité. Et là, plus encore qu'aujourd'hui on va devoir être prudents parce qu'on va devoir gérer notre enquête en fonction de l'argent alloué par l'État. C'est le grand souci et le malaise évidemment puisque si on veut museler les enquêtes du juge, il suffit simplement de donner un petit budget »³⁰¹.

2.3. De nombreuses contraintes juridiques

Dans un état démocratique, de nombreuses contraintes juridiques entourent les pratiques quotidiennes des autorités judiciaires et des services de police. C'est, à plus forte raison, le cas en matière de traçabilité numérique. *« Celle-ci est extrêmement encadrée. D'une manière générale, nous devons assurer le respect de procédures et garanties légales extrêmement balisées »³⁰².* Ainsi, la multitude de normes juridiques constitue assurément un écueil à l'établissement d'une société de surveillance. Le postulat essentiel de ce troisième obstacle est formulé par Vincent Francis dans l'extrait suivant :

« La jurisprudence des cours et tribunaux en Belgique est extrêmement sévère vis-à-vis de tout dérapage juridique. La légalité des traces numériques est souvent remise en question par les cours et tribunaux. Il y a vraiment un travail de la justice de fond. La jurisprudence est assez stricte et quand on observe la loi, il y a un certain nombre de garde-fous qui sont indispensables. Je pense que si ce n'est pas directement pour éviter la surveillance de masse, cela a un impact positif sur cet aspect »³⁰³.

³⁰¹ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

³⁰² Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

³⁰³ Entretien avec Monsieur Vincent Francis réalisé le 22 mars 2016.

De nombreuses normes juridiques ont été adoptées par le législateur belge, dont l'objectif n'est, a priori, pas de lutter contre l'implantation d'une société de surveillances sous le prisme de la traçabilité. Cependant, par certains droits fondamentaux qu'elles garantissent, ces normes préviennent indirectement un tel établissement. Dans ce cadre, un droit fondamental est celui garantissant le respect de la vie privée. S'il a été abordé lors de la présentation des critères d'application d'une mesure de traçabilité, ce droit constitue plus largement un garde-fou indispensable contre les possibles dérives liberticides d'une surveillance généralisée. « Depuis les trente-cinq dernières années, la protection de la vie privée s'est répandue dans le monde comme une réponse par les pays et les organismes internationaux aux menaces perçues provenant des activités publiques et privées qui ont souvent à leur disposition des moyens technologiques sophistiqués pour le traitement des données personnelles »³⁰⁴. Ainsi, la protection légale de la vie privée a, en Belgique, une véritable incidence sur les pratiques de surveillance. Nous pouvons l'illustrer par l'extrait suivant : « *Nous ne faisons pas de proactivité lorsque nous avons recours aux entreprises privées. On ne va pas aller interroger la Fnac ou Media Mark pour avoir le top 10 des clients qui achètent X ou Y choses par mois au niveau du magasin. On ne peut pas le faire. Cela ne va jamais être de la pêche !* »³⁰⁵.

Le droit au respect de sa vie privée ne constitue pas l'unique contrainte juridique contre le développement au sein de la société d'une surveillance généralisée. D'autres normes, plus informelles, s'inscrivent dans la même lignée. L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques instaure, par exemple, une obligation de conserver certaines données de télécommunication³⁰⁶. Cette rétention n'est toutefois autorisée que pour une durée limitée ; celle-ci étant fixée à une année. Pour la juge d'instruction Martine Michel, une telle rétention représente une barrière juridique empêchant pleinement le recours aux nouvelles technologies de traçabilité. « *Les opérateurs de téléphonie mobile détiennent les informations comme la localisation des télécommunications pendant un an, alors que techniquement je suis certaine qu'ils peuvent en garder pendant beaucoup plus longtemps. Ils veulent même limiter le délai jusqu'à un mois, mais pour l'instant on tient bon...* »³⁰⁷. Passé cette échéance, l'information n'est plus disponible pour les autorités judiciaires dans le cadre d'une enquête pénale. Comment pourrions-nous dès lors concevoir l'établissement d'une société de surveillance à partir de traces conservées pendant une période aussi courte ?

³⁰⁴ SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 78.

³⁰⁵ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

³⁰⁶ *Voy.* Point 3.1.2.3. p. 53.

³⁰⁷ Entretien avec Madame Martine Michel réalisé le 8 mars 2016.

L'usage d'une technologie numérique de traçabilité s'inscrit donc dans un contexte juridique restreignant. Assurément, une série de normes légales encadrent indirectement les pratiques de surveillance dans lesquelles s'inscrit un tel usage. Outre la vie privée et la rétention limitée de données, notons à titre illustratif que « *la Belgique a légalement prévu que ce n'est que le juge d'instruction, garant des libertés individuelles, qui peut décider de la mise en œuvre une telle surveillance. Ce n'est pas un policier ou le procureur du roi qui peuvent la réaliser* »³⁰⁸. Seul un juge d'instruction est donc autorisé, sous couvert de la loi, à mettre en place des mesures intrusives de surveillance. Confronté à ces nombreuses contraintes juridiques non-exhaustives, l'établissement d'une société de surveillance ne peut ainsi être constaté.

2.4. L'adaptation des délinquants aux mesures judiciaires de traçabilité

Une surveillance, diffuse et globale, par le biais de la traçabilité numérique suppose de pouvoir recueillir un certain nombre de traces disséminées par une population particulière. Localiser un individu par l'usage de son téléphone portable ou de sa carte bancaire peut ainsi être déterminé au regard de ces informations collectées par les acteurs judiciaires. Toutefois, « *les délinquants sont de plus en plus au courant de la géolocalisation de leur appareil* »³⁰⁹. Les autorités judiciaires et les services de police se trouvent dès lors placés devant un écueil majeur : « *les suspects n'envoient plus de sms par peur de laisser des traces. Certaines techniques sont utilisées par les délinquants à l'heure actuelle sans que l'on puisse en tracer les communications ! Si on veut commander six tonnes de cannabis, il vaut mieux le faire par Skype que par sms. Il y a des méthodes qui ne laissent donc plus de traces* »³¹⁰. Par conséquent, l'adaptation des délinquants aux mesures judiciaires de traçabilité, comme observé à travers les propos des juges d'instruction, constitue ainsi un dernier obstacle aux pratiques de surveillance et de suivi à grande échelle de l'individu.

Plus précisément, de nombreuses démarches délictueuses s'inscrivent, pour se dérober du regard de la surveillance, dans un processus d'anonymisation de l'individu par la suppression de ses traces. « *Il existe des systèmes complexifiant considérablement le processus d'identification par le relevé de traces, le rendant impossible pour la justice selon des raisons*

³⁰⁸ Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

³⁰⁹ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

³¹⁰ Entretien avec Madame Christine Dierick réalisé le 6 avril 2016.

pratiques »³¹¹. Cette suppression des traces est indubitablement motivée par le recours aux instruments de traçabilité numérique des acteurs judiciaires et dont la fréquence croissante incite les délinquants à s'adapter. Nous pouvons également observer ce phénomène dans les propos tenus par Verena Reul : « *Les vrais truands ne prennent plus leur gsm en réaction aux méthodes policières. Les truands s'adaptent à ces techniques. Ils ont véritablement un coup d'avance sur la justice qui ne dispose pas des moyens pour lutter efficacement contre toute forme de criminalité* »³¹². Stéphane Kerkhofs établit le même constat : « *Maintenant, un investissement des délinquants, c'est de ne plus être traçable par les services de police et de brouiller les pistes au maximum en changeant de téléphone, par exemple. Il existe des programmes de brouillage comme Tor* »³¹³.

L'usage de dispositifs permettant de se mouvoir dans la société sans laisser de traces est, en définitive, une stratégie de plus en plus prise en compte par ces individus. De telles méthodes sont à l'image de la traçabilité ; aussi diverses que variées. Se procurer anonymement une carte SIM en est un exemple. Le système de téléphone via Internet, comme Skype, est un autre moyen pour échapper à la curiosité policière³¹⁴. Tous ont comme point commun d'empêcher la traçabilité de la personne. De cette manière, il est possible pour les personnes soumises à une enquête pénale de se soustraire au contrôle et à la vigilance des acteurs judiciaires. À cet égard, l'adaptation des délinquants à ces mesures judiciaires s'érige, *in fine*, en un véritable obstacle à l'encontre de la société de surveillance.

³¹¹ Entretien avec Monsieur Jean-François Joris réalisé le 15 mars 2016.

³¹² Entretien avec Madame Verena Reul réalisé le 13 avril 2016.

³¹³ Entretien avec Monsieur Stéphane Kerkhofs réalisé le 15 mars 2016.

³¹⁴ F.-B. HUYGHE, « Téléphonie mobile : capter la vie numérique des autres », *Hermès, La Revue*, 2009, vol. 1, p. 82.

3. Conclusion

A la question qui sert de titre à cette partie de notre travail et lui a en grande partie servi de moteur, nous devons donc répondre par la négative. De nombreux obstacles, fussent-ils formels tels les prescrits légaux et les limitations imposées aux acteurs du monde judiciaire ou périphériques des pratiques de surveillance comme le volume de données à traiter, les marges budgétaires restreintes pour ce faire et la capacité d'adaptation non-négligeable des personnes visées ou se sentant visées par la surveillance, viennent circonscrire le phénomène tant et si bien que l'expression « société de surveillance » semble inadaptée pour le décrire, du moins vue par le biais de la traçabilité numérique.

Plutôt qu'une surveillance indiscriminée pratiquée par les autorités judiciaires, la réalité nous montre qu'une certaine restriction, involontaire peut-être, préside à l'usage des moyens mis à leur disposition et empêche l'avènement d'une société qui soit toute entière épiée et contrôlée. Ne perdons cependant pas de vue que lesdits facteurs sont sujets à des changements, qui eux-mêmes peuvent induire des évolutions radicales quant à la place prise par la surveillance dans la société. Les marges budgétaires, par exemple, sont des décisions purement politiques : si un état démocratique réclame plus de sécurité, l'appareil judiciaire peut *in fine* voir cette contrainte reculer, et la surveillance en profiter. Les limitations juridiques sont également susceptibles de changer de la même façon.

Cette situation nous semble encore plus interpellante dans le contexte actuel où le sentiment de danger et le désarroi du citoyen n'ont jamais été aussi prononcés. En tout état de cause, une certaine circonspection et une attention rigoureuse à l'égard des développements futurs en la matière sont de mise ; de même qu'encadrer la surveillance, si les facteurs précités n'y suffisent plus.

Conclusion générale

Aux États-Unis comme en Europe, mais également de plus en plus en Asie, en Amérique latine et au Moyen-Orient, la surveillance généralisée fait partie intégrante de notre mode de vie³¹⁵. D'aucuns estiment nécessaire, pour contrer toute menace potentiellement nuisible, l'intensification d'une surveillance, facilitée notamment par les nouvelles technologies numériques de traçabilité. Pour justifier cet accroissement de mesures toujours plus liberticides, nombreux sont les plaidoyers des autorités étatiques reposant sur une motivation particulière : la captation de données disséminées après l'usage de ces instruments numériques, procurant aux autorités judiciaires et services de police de multiples renseignements sur les agissements et déplacements de l'Homme. Ainsi, de telles technologies de traçabilité seraient particulièrement « bien adaptées à notre société au point de pouvoir en faire, selon un certain nombre de commentateurs, une véritable société de surveillance »³¹⁶.

Qu'est ce que la Société de Surveillance ? Ce concept étant perçu comme une composante aussi substantielle qu'opaque au sein de notre société contemporaine, notre étude a eu pour principal objectif d'expliciter ses tenants et aboutissants afin de pouvoir apprécier par la suite son éventuel établissement dans les arrondissements judiciaires en Wallonie. À cet effet, nous avons emprunté un cheminement particulier : analysant au préalable cette société au niveau international, nous avons poursuivi notre étude des pratiques judiciaires de traçabilité numérique au niveau local.

Nous nous sommes d'abord attachés à l'analyse des tendances sous-jacentes de la Société de Surveillance. En effet, il est apparu qu'un tel phénomène était implicitement ajusté par l'action de facteurs universels. Que nous songeons au risque, à l'impact d'événements traumatisants, à l'apport de multiples technologies à caractère militaire ou développées par une industrie en pleine expansion ainsi qu'à l'action, volontaire ou non, des citoyens... La littérature scientifique sur laquelle nous nous sommes appuyés le démontre pleinement ; outre leur apport individuel, c'est par la conjugaison de l'ensemble de ces facteurs que ces derniers jouent indéniablement un rôle fondamental dans les pratiques mondiales de surveillance et modèlent, par conséquent, la société dans laquelle nous vivons.

³¹⁵ D. LYON, « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », *op. cit.*, p. 90.

³¹⁶ C. LAVAL, *op. cit.*, p. 50.

Ensuite, nous avons procédé à l'analyse de la Société de Surveillance en tant que phénomène global aux frontières nullement correspondant à des limites territoriales classiques. Notre présentation se voulait générale : un tel phénomène présente assurément une dimension collective eu égard à la nature de la surveillance et à son caractère immanent aux rapports sociaux. Ce sont d'ailleurs, comme nous avons pu le constater, ces derniers qui se retrouvent au cœur des différentes pratiques de surveillance ; d'autant plus qu'elles ont pour objectif de contrôler, gérer, influencer un groupe d'individus. Pour ce faire, divers auteurs repris dans notre étude pointent plusieurs mécanismes-clés de cette société comme le partage de l'information, le détournement d'usage et le tri social. Tous ont ainsi pour objectif de concourir à la suppression des menaces au sein de la société par un partage de données détournées de leurs fonctions et objectifs premiers, permettant une catégorisation toujours plus importante des individus.

Nous pensons que de telles pratiques sont éminemment contestables ! Nous ne pouvons perdre de vue les dérives qui découlent implicitement de ces mécanismes. Devons-nous par exemple tolérer la mise en place dans notre société, consécutivement à des attaques terroristes, d'une surveillance accrue des populations musulmanes au motif de leur simple appartenance religieuse ? Si « ceux qui n'ont rien à se reprocher n'ont rien à craindre », certains effets pervers de tels mécanismes-clés viennent directement s'opposer à cet habituel refrain en matière de surveillance.

Par ailleurs, au sein de cette société de surveillance, la mise en œuvre et le développement de tels mécanismes dépendent pleinement des nouvelles technologies, et notamment celles liées à la traçabilité numériques. De nombreux auteurs et chercheurs estiment de la sorte que ces dernières ont contribué à changer « le visage » de la surveillance. Nous avons dès lors porté, lors de cette analyse, une attention accrue à ces dispositifs technologiques. C'est d'ailleurs dans cette phase spécifique de notre étude que nous avons orienté nos recherches vers un examen au niveau local – celui des arrondissements judiciaires en Wallonie – des pratiques de surveillance par le biais de la traçabilité des comportements humains. Celui-ci nous a permis de démontrer qu'un tel recours n'est pas libre de toute contrainte. L'emploi d'une technologie de traçabilité est ainsi soumis à différents critères au sein d'un champ d'application particulier.

Ces développements sur les pratiques judiciaires nous ont enfin permis d'apporter une réponse à notre interrogation centrale : vivons-nous présentement dans une société de surveillance ? À cette question, nous avons répondu par la négative au terme de notre étude. En effet, nous estimons que l'usage par les acteurs judiciaires des technologies numériques de traçabilité n'instaure pas dans les limites territoriales de nos recherches une telle société. Outre les critères d'application d'un tel usage, nous avons déterminé qu'une série d'obstacles s'érige à l'encontre de son établissement. Ces derniers sont multiples et ont principalement trait au manque de moyens humains et financiers, aux prescrits légaux et à la faculté d'adaptation des délinquants aux mesures judiciaires. Nous nous sommes ainsi aperçus que de tels obstacles viennent encadrer et limiter implicitement l'impact des différentes pratiques de surveillances.

Néanmoins, nous nous devons d'insister pleinement sur le fait que notre contribution représente une photographie contemporaine d'un cadre délimité : tant ce cadre que les pratiques existant en dehors de celui-ci sont soumis à une certaine fluctuation. Il est dès lors probable qu'en raison de certaines circonstances, l'existence et l'établissement d'une société de surveillance puissent apparaître de manière insidieuse dans nos contrées occidentales, traitant chaque citoyen comme un suspect potentiel aux droits amoindris. Par conséquent, nous appelons vivement à une attention soutenue envers ces changements sociaux.

Bibliographie

Textes législatifs

Arrêté Royal du 8 février 2016 modifiant l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

Code du 28 février 2013 relatif au droit économique.

Code du 17 novembre 1808 relatif à l'instruction criminelle.

Directive du 15 mars 2006 relative à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication.

Loi du 13 juin 2005 relative aux communications électroniques.

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Ouvrages

ALBERGANTI M., *Sous l'œil des puces : la RFID et la démocratie*, Arles, Actes Sud, 2007.

AMNESTY INTERNATIONAL USA, *Threat and Humiliation : Racial Profiling, Domestic Security and Human Rights in the USA*, New York, Amnesty International USA, 2004.

BECK U., *La société du risque : sur la voie d'une autre modernité*, Paris, Aubier, 2002.

BERTHOUD G., « L'horizon d'une surveillance omniprésente ? », *Revue européenne des sciences sociales*, 2002, pp. 155-168.

CONGRESSIONAL RECORD, *Proceedings and debates of the 110th congress : first session*, Vol. 153, Pt. 26, 17 December 2007.

DANDEKER C., *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge, Polity press, 1990.

DELBECQUE E., *Idéologie sécuritaire et société de surveillance : le storytelling du XXI^e siècle*, Paris, Vuibert, 2015.

DE VALKENEER C., *Manuel de l'enquête pénale*, 4^e éd., Bruxelles, Larcier, 2011.

DUPONT B., « Hacking the Panopticon: distributed online surveillance and resistance », In *Surveillance and governance: Sociology of Crime Law and Deviance*, éd. par Mathieu Deflem, Bingley, Emerald, 2008.

ELLUL J., *La Technique ou l'Enjeu du siècle*, Economica, Paris, 1990.

FOREST D., *Abécédaire de la société de surveillance*, Paris, Syllepse, 2009.

GAILLARD M., « Nouvelles technologies de l'information et de la communication et protection des libertés du citoyen », In *Les libertés individuelles à l'épreuve des NTIC*, sous la dir. de Marie-Christine Piatti, Lyon, Presses universitaires de Lyon, 2001.

HAGGERTY D. K., « Surveillance, crime and the police », In *The Routledge Handbook of Surveillance Studies*, éd. par Kirstie Ball, Kevin D. Haggerty et David Lyon, Abingdon, Routledge, 2012.

HAGGERTY D. K. & ERICSON R., « Les technostructures militaires du maintien de l'ordre », In *La militarisation des appareils policiers*, sous la dir. de Frédéric Lemieux et Benoît Dupont, Lévis, Les Presses de l'Université Laval, 2005.

HERMITTE M.-A., « La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise », In *Traçabilité et responsabilité*, sous la dir. de Philippe Pédrot, Paris, Economica, 2003.

HUYGHE F.-B., « Téléphonie mobile : capter la téléphonie des autres », *Hermès, La Revue*, 2009, vol.1, pp. 79-84.

JABLONKA I., « Aux origines de la surveillance de masse. Entretien avec Sophie Cœuré », In *La Vie des idées*, 12 janvier 2016.

LAVAL C., « Surveiller et prévenir. La nouvelle société panoptique », *Revue du MAUSS*, 2012, vol.2, pp. 47-72.

LEMAN-LANGLOIS S., « Introduction : Qu'est-ce que la surveillance ? », In *Sphères de surveillance*, sous la dir. de Stéphane Lemana-Langlois, Montréal, Presses de l'Université de Montréal, 2011.

LEVALLOIS-BARTH C., « La géolocalisation : un nouvel impératif », *Hermès, La Revue*, 2009, vol.1, pp. 99-104.

LUPTON D., *Risk*, 2^e éd., Londres, Routledge, 2003.

LYON D., « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », In *Au nom du 11 septembre... : les démocraties à l'épreuve de l'antiterrorisme*, sous la dir. de Didier Bigo, Laurent Bonelli et Thomas Deltombe, Paris, La Découverte, 2008.

LYON D., « Identity cards : social sorting by database », *Oxford Internet Institute, Internet Issue Brief No. 3*, 2004.

LYON D., *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003.

LYON D., « Surveillance as social sorting : computer codes and mobile bodies », In *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003.

LYON D., *The electronic eye: the rise of surveillance society*, Cambridge, Polity press, 1994.

MARQUIS G., « Private security and surveillance : from the dossier « society » to database networks », In *Surveillance as Social sorting : privacy, risk and digital discrimination*, éd. par David Lyon, New York, Routledge, 2003.

MARX T. G., « La société de sécurité maximale », *Déviance et société*, 1988, vol.12, pp. 147-166.

MERZEAU L., « Du signe à la trace : l'information sur mesure », *Hermès, La Revue*, 2009, vol.1, pp. 21-29.

NEYLAND D. & KROENER I., « New technologies, security and surveillance », In *Routledge Handbook of Surveillance Studies*, éd. par Kirstie Ball, Kevin D. Haggerty et David Lyon, Abingdon, Routledge, 2012.

NORRIS C. & ARMSTRONG G., *The Maximum Surveillance Society – The Rise of CCTV*, Oxford et New York, Berg, 1999.

PERETTI-WATEL P., *Sociologie du risque*, Paris, Armand Colin, 2000.

POUPART J., « L'entretien de type qualitatif: considérations épistémologiques, théoriques et méthodologiques », In *La recherche qualitative. Enjeux épistémologiques et méthodologiques*, Montréal, Gaëtan Morin, 1997.

RAMONET I., *L'empire de la surveillance*, Paris, Galilée, 2015.

SADIN E., *Surveillance globale : enquête sur les nouvelles formes de contrôle*, Paris, Climats, 2009.

SIMON J., « Le parti du risque », *Vacarme*, 2007, vol. 3, pp. 16-20.

STANLEY J., *The Surveillance-Industrial Complex: How the American Government is conscripting businesses and individuals in the construction of a Surveillance Society*, Washington DC, ACLU, 2004.

STEINHARDT B. & STANLEY J., *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, Washington DC, ACLU, 2003.

SURVEILLANCE STUDIES NETWORK, *A Report on the Surveillance Society*, Knowledge House (Mark Siddoway), 2006, p. 11

TRÉVIDIC M., *Au cœur de l'antiterrorisme*, Paris, JC Lattès, 2011.

TÜRK A. & PIAZZA P., « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Culture & Conflits*, 2009, pp 115-134.

TZANOU M., « The UE as an emerging surveillance society : the function creep case study and challenges to privacy and data protection », *Vienna Online J. on Int'l Const. L.*, 2010, vol. 4.

VADROT C.-M., *La grande surveillance : caméras, ADN, portables, Internet...*, Paris, Seuil, 2007.

VALLET C., « Fichés jusqu'au ciel ? », *Alternatives Internationales*, 2015, vol. 3.

VAN CAMPENHOUDT L. & QUIVY R., *Manuel de recherche en sciences sociales*, 4^e éd., Paris, DUNOD, 2013.

Articles de presse

BRIDLE J., « All cameras are police cameras », *The Nor*, mis en ligne le 7 novembre 2014, consulté le 18 mai 2016.

Disponible sur : <http://shorttermmemoryloss.com/nor/2014/11/07/all-cameras-are-police-cameras/>.

DREYFUS S., « Un péage en plein cœur de Londres », *Le Monde*, mis en ligne le 17 février 2003, consulté le 18 mai 2016.

Disponible sur : http://www.lemonde.fr/archives/article/2003/02/17/un-peage-en-plein-c-339-ur-de-londres_309533_1819218.html?xtmc=congestion_charge_zone&xtr=13.

ELECTRONIC PRIVACY INFORMATION CENTER, « Northwest Airlines Gave NASA Personal Info on Millions of Passengers; Disclosure Violated Privacy Policy », *Press release*, mis en ligne le 18 janvier 2004, consulté le 16 mai 2016.

Disponible sur : <https://epic.org/privacy/airtravel/nasa/pr1.18.04.html>.

EUDES Y., « Pourquoi l'accord Safe Harbor sur les données personnelles cristallise les tensions ? », *Le Monde*, mis en ligne le 25 septembre 2015, consulté le 23 mars 2016.

Disponible sur : http://www.lemonde.fr/pixels/article/2015/09/25/pourquoi-l-accord-safe-harbor-sur-les-donnees-personnelles-cristallise-les-tensions_4771879_4408996.html.

HEALY P., « colleges giving probers data on foreign students' finances », *The Boston Globe*, mis en ligne le 3 octobre 2001, consulté le 16 mai 2016.

Disponible sur : <https://www.highbeam.com/doc/1P2-8673165.html>.

IGGULDEN A., « CCTV channel beamed to your home », *The Telegraph*, mis en ligne le 10 mai 2006, consulté le 29 mars 2016.

Disponible sur : <http://www.telegraph.co.uk/news/uknews/1517836/CCTV-channel-beamed-to-your-home.html>.

MARRON K., « New Crime Fighter Rides Along with Cops in Cruisers », *The Globe and Mail*, mis en ligne le 23 février 2001, consulté le 8 avril 2016.

Disponible sur : <http://www.theglobeandmail.com/incoming/new-crime-fighter-rides-along-with-cops-in-cruisers/article25442600/>.

MAUSSION C., « Des hypers super mobiles », *Libération*, mis en ligne le 12 octobre 2006, consulté le 10 avril 2016.

Disponible sur : http://www.liberation.fr/futurs/2006/10/12/des-hypers-super-mobiles_54035.

NORMAND J.-M., « Bientôt des drones de surveillance pour la préfecture de police », *Le Monde*, mis en ligne et consulté le 21 mars 2016.

Disponible sur : <http://drones.blog.lemonde.fr/2016/03/31/la-prefecture-de-police-commande-des-drones-de-surveillance/>.

ORR J., « Police send ‘spy drone’ into the skies », *The Guardian*, mis en ligne le 21 mai 2007, consulté le 28 mars 2016.

Disponible sur : <http://www.guardian.co.uk/crime/article/0,,2084801,00.html>.

SINGEL R., « JetBlue shared passenger data », *Wired*, mis en ligne le 18 septembre 2003, consulté le 16 mai 2016.

Disponible sur : <http://www.wired.com/2003/09/jetblue-shared-passenger-data/>.

STEPANEK M., « Weblining », *Bloomberg*, mis en ligne le 3 avril 2000, consulté le 7 avril 2016.

Disponible sur : <http://www.bloomberg.com/news/articles/2000-04-02/weblining>.

STROOBANTS J.-P., « Accord sur le PNR, le fichier qui regroupera les données des passagers aériens en Europe », *Le Monde*, mis en ligne le 10 décembre 2015, consulté le 7 février 2016.

Disponible sur : http://www.lemonde.fr/europe/article/2015/12/10/accord-crucial-sur-le-fichier-europeen-des-passagers-aeriens_4829041_3214.html.

Sites Internet

<http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-devant-le-parlement-reuni-en-congres-3/>, consulté le 17 février 2016.

<http://www.sagem.com/fr/societe>, consulté le 23 février 2016.

<http://www.gouvernement.fr/partage/5883-prorogation-de-l-etat-d-urgence-discours-de-manuel-valls-devant-l-assemblee-nationale>, consulté le 8 mars 2016.

http://tetrad.com/pub/documents/psyteadv_clusters.pdf, consulté le 13 mars 2016.

<https://www.privacycommission.be/sites/privacycommission/files/documents/protection-donnees-a-caractere-personnel-en-belgique.pdf>, consulté le 28 mars 2016.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>, consulté le 2 avril 2016.

<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52011PC0032>, consulté le 11 avril 2016.

<http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0099&language=FR>, consulté le 14 avril 2016.

<http://www.acxiom.fr/big-data-et-datamining/>, consultée le 23 avril 2016.

La Société de Surveillance ; mythe ou réalité au sein des pratiques judiciaires de traçabilité numérique ?

Promoteur : Professeur Marie-Sophie Devresse

Nébuleuse et opaque, la Société de Surveillance est un concept flou qui s'introduit à grand bruit dans les questions sociétales en Occident. Le contexte n'y est pas étranger ; les lendemains mornes et exsangues d'attaques terroristes entraînent le souhait d'accroître les pratiques de surveillance déjà existantes. Les développements de nouvelles technologies en matière de traçabilité numérique favorisent également cette introduction. En effet, le téléphone portable, la carte bancaire et bien d'autres instruments offrent à divers acteurs, étatiques ou judiciaires, de nombreuses données sur les agissements de l'Homme. Dès lors, vivons-nous dans une société de surveillance ? C'est en vue de répondre à cette question que nous avons tenté, dans le cadre de ce mémoire, de rendre compte des différentes pratiques de traçabilité numérique mises en œuvre par la justice pénale. C'est au sein de ce cadre restreint que nous avons ainsi abordé la Société de Surveillance.