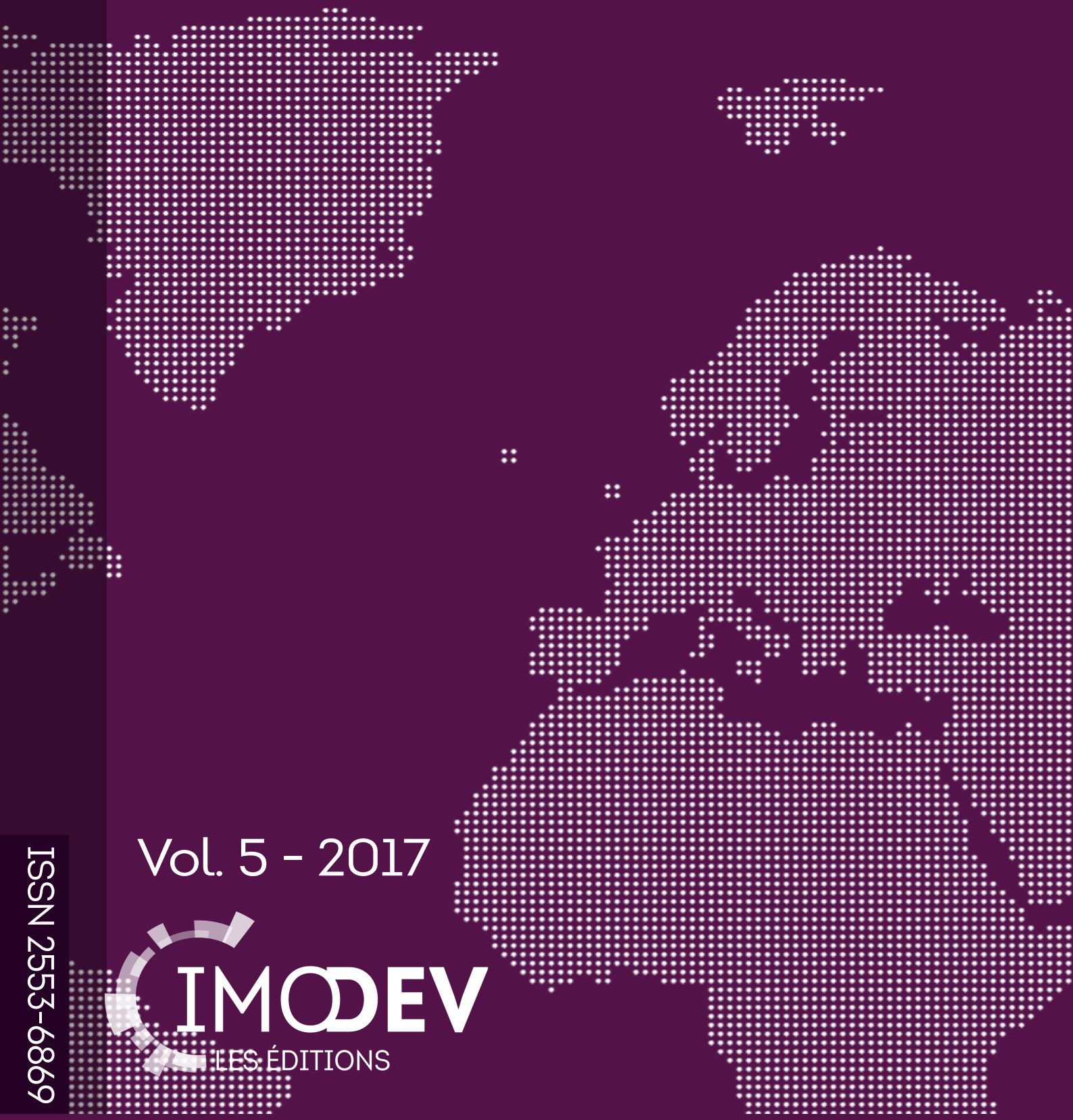
INTERNATIONAL JOURNAL OF **OPEN GOVERNMENTS**

REVUE INTERNATIONALE DES **GOUVERNEMENTS OUVERTS**



Vol. 5 - 2017

ISSN 2553-6869

IMODEV
LES ÉDITIONS

International Journal of Open Governments
Revue internationale des gouvernements ouverts

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6869

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale des Gouvernements ouverts (RIGO)/ the International Journal of Open Governments** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Open Governments / Revue Internationale des Gouvernements ouverts (RIGO)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

and 2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

ADMINISTRATION ET COLLECTE DE DONNÉES PERSONNELLES SUR INTERNET ET LES RÉSEAUX SOCIAUX : À LA RECHERCHE D'UN CADRE JURIDIQUE ADÉQUAT[1]

par **Patricia JONASON**, Maître de Conférences à l'Université de Södertörn, Stockholm.

L'explosion de l'utilisation d'Internet et des réseaux sociaux modifie, peu s'en faut, les habitudes des individus et les relations et modes de communication interpersonnels. Ces bouleversements technologiques impactent également les pratiques des administrations dans leurs relations avec les citoyens. En témoigne le nombre toujours plus grand d'autorités publiques[2] ayant créé, qui un compte Facebook, qui un blog, comme plateforme de communication avec les administrés[3]. Mais encore, l'administration se sert de manière croissante d'Internet et des réseaux sociaux – ces derniers étant alimentés par les individus eux-mêmes – pour collecter des informations sur les administrés. Cette dernière pratique, sur laquelle portera la présente analyse, trouve une illustration concrète dans une affaire soumise à l'Ombudsman parlementaire suédois concernant la recherche d'informations, faite par les services sociaux de la bourgade de Hultsfred, sur le compte Facebook d'une administrée[4]. Cette affaire (que par la suite nous nommerons affaire Facebook), qui a donné lieu, en janvier 2015, au rendu par l'instance suédoise d'une décision, était la suivante : Madame Linda S. avait déposé une plainte à l'encontre d'un agent des services sociaux de sa ville pour atteinte à sa vie privée. La plaignante reprochait à l'assistante sociale, en charge de son dossier de demande de renouvellement d'aides sociales, d'avoir récolté sur des réseaux sociaux des informations la concernant

[1] Cet article, qui se propose de contribuer à une réflexion générale sur les risques, pour la vie privée et la démocratie, que peuvent engendrer pour les citoyens les nouvelles pratiques de l'administration générées par les transformations technologiques et sociétales, s'inscrit dans le cadre d'un projet de recherche « *La vie privée – aspect caché de la démocratie suédoise. Une étude juridique et historique de la recherche d'un équilibre entre la transparence er la protection de la vie privée en Suède* » (« Privatlivet – den undanskymda aspekten i svensk demokrati - En juridisk och historisk undersökning om avvägningen mellan öppenhet och privatliv i Sverige »), financé par le Conseil suédois de la Recherche.

[2] En Suède, par exemple, l'Agence nationale de la protection environnementale détient quatre comptes Facebook. Les Universités, les bibliothèques, les communes, l'Administration nationale des tribunaux, l'Autorité de la concurrence, pour ne citer qu'elles, détiennent toutes des comptes Facebook.

[3] Ce peut être le cas, lorsque, pour accroître sa proximité d'avec les citoyens, la police les informe de ses activités quotidiennes, ou bien prodigue à ceux-ci des conseils pour les aider à se protéger de la criminalité, ou encore lance un appel à témoins.

[4] Décision de l'Ombudsman nº 2611-2013 du 15 janvier 2015.

personnellement[5]. C'est lors d'un entretien avec cet agent, et en découvrant parmi les pièces de son dossier administratif des reproductions de photographies postées sur son propre compte Facebook et sur le blog d'une de ses amies, que Madame S. a réalisé quel procédé avait été utilisé pour rassembler des informations à son sujet. Elle avait alors éprouvé, comme elle l'a rapporté à l'Ombudsman, le sentiment désagréable d'avoir été « épiée » et également que la fonctionnaire chargée de son dossier avait « mis son nez » dans sa sphère privée[6].

La pratique administrative consistant à collecter des informations personnelles sur Internet, et les réseaux sociaux en particulier, constitue sans aucun doute un moyen de rendre plus efficaces les tâches de l'administration. Elle permet entre autres, dans un cas comme celui qui vient d'être présenté, la simplification des nécessaires vérifications des sources de revenus des demandeurs, lesquelles doivent être effectuées avant la prise de décision du versement d'une aide et de son montant. Toutefois, les investigations administratives dans le champ du Cyberespace n'en sont pas moins potentiellement attentatoires aux fondements de la démocratie. À côté des ingérences dans la vie privée des citoyens directement concernés par de telles mesures, une utilisation des plateformes et outils numériques par les administrations est susceptible d'entamer la confiance du public dans les organes de l'État. Ceci risque, à terme, de provoquer chez des citoyens gagnés par la méfiance à l'égard d'une administration par trop « voyeuse », une autolimitation de leurs libertés et, par extension, de menacer le pluralisme des expressions d'opinion comme des modes de vie.

Face aux risques d'atteintes à la vie privée des citoyens, nul doute qu'il soit besoin d'un encadrement juridique contraignant des investigations administratives sur Internet (1). Un tel dispositif de *hard law* n'est toutefois pas suffisant, eu égard à la complexité de la question et à l'ampleur des enjeux en présence. Il doit être complété par un dispositif au caractère de *soft law* (2) ayant pour fonction de guider les agents de l'administration dans l'application au cas par cas des règles contraignantes, et de leur faire prendre conscience des enjeux privés et collectifs inhérents à la pratique des investigations administratives « cyberspaciennes ».

[5] Les photos en question montraient entre autres une portée de chiots et des chevaux, soit des éléments susceptibles d'être pris en compte par l'administration dans le calcul de la situation économique d'un demandeur d'aide sociale.

[6] Laissons de côté la question de savoir si la fonctionnaire mise en cause a, comme elle l'a soutenu, accédé à des données rendues publiques par l'intéressée du fait de la non utilisation par celle-ci des paramètres de sécurité mis à disposition par Facebook ou si, comme l'affirme Madame S., la fonctionnaire a subrepticement accédé au compte Facebook de l'administrée par le biais d'une « amie » numérique. Ce différend, sur lequel d'ailleurs l'Ombudsman n'a pas voulu se prononcer, ne constitue pas l'enjeu central de la discussion.

§ 1 – UN CADRE JURIDIQUE POUR PARTIE CONTRAIGNANT[7]

Comment les investigations administratives à l'aide d'Internet, pratique d'origine récente, sont-elles appréhendées par le droit national ? C'est ce que nous verrons, dans un premier temps, à partir de l'exemple suédois (A), avant d'aborder les exigences posées en la matière par les textes d'origine européenne, la législation de l'Union européenne sur la protection des données personnelles et la Convention européenne des droits de l'homme (B).

A) Le cadre national : l'exemple suédois

Le droit suédois est, à l'heure actuelle, dépourvu de dispositif régulant la faculté des administrations de procéder à la recherche et à la collecte d'informations sur Internet et les réseaux sociaux. Toutefois, les dispositions de la loi sur l'aide sociale consacrées aux investigations « traditionnelles » opérées par les services sociaux, et même si elles ne couvrent pas le phénomène dans toute sa singularité, fournissent un certain cadre aux nouvelles pratiques d'investigation (1).
De façon plus générale, deux principes que l'on retrouve dans le droit suédois seraient à même d'encadrer les investigations administratives effectuées à l'aide d'Internet et des réseaux sociaux. Il s'agit du principe d'objectivité, tiré du droit constitutionnel (2) et du principe du respect de la vie privée, principe mi-constitutionnel, mi-législatif (3).

1) L'application, par analogie, des dispositions sur les investigations traditionnelles tirées de la loi sur l'aide sociale

La loi suédoise sur l'aide sociale[8], adoptée à une époque où Internet n'existait pas, repose, comme le rappelle l'Ombudsman dans l'affaire Facebook, sur le principe que toutes les activités des services sociaux, y compris les investigations, doivent être entreprises en tenant compte du droit des citoyens à participer à la prise des décisions les concernant et en respectant leur intégrité[9] (l'article 3.3 du chapitre 1). Il en découle, premièrement, que l'administration doit tenir compte, pour décider des mesures d'investigation à mettre en œuvre, de la mise en balance des atteintes à l'intégrité de la personne susceptibles d'être produites par les investigations, d'une part, et des intérêts poursuivis par l'administration, d'autre part[10]. Il en découle, deuxièmement, qu'en principe les services sociaux sont tenus de ne pas collecter d'informations auprès de tiers, à moins que l'intéressé n'y

[7] Nous nous contenterons ici de remarques et réflexions assez générales. Un examen plus approfondi et détaillé est entrepris dans le cadre du travail de recherche susmentionné (voir la note 1).
[8] Socialtjänstelagen (2001:453).
[9] Le concept d'intégrité étant plus vaste que celui de protection de la vie privée.
[10] Prop 1979/80:1, Partie A., p. 400 et 562, cité dans la décision Facebook, p. 5.

consente[11]. Que valent ces principes, institués pour les investigations effectuées à l'aide de méthodes traditionnelles, dans le contexte nouveau de la collecte d'informations sur Internet et les réseaux sociaux ? La réponse qui se dégage de la décision Facebook n'est pas très claire sur ce point. En effet, l'Ombudsman indique que lorsque les informations sont rendues publiques en étant publiées sur un blog ou sur une page Facebook, il n'existe pas *a priori* d'obstacle formel à ce que les services sociaux procèdent à leur collecte sans le consentement des administrés[12]. L'Ombudsman affirme cependant que les principes susmentionnés découlant de l'article 3.3 du chapitre 1 de la loi sociale ont vocation à s'appliquer à la collecte de données sur les réseaux sociaux[13]. Autrement dit, il semblerait que la loi sur l'aide sociale qui, bien que non conçue pour réguler la collecte d'information sur Internet et les réseaux sociaux, puisse constituer partiellement, en ce qui concerne les agents des services sociaux, un cadre légal pour ce genre de pratiques.

2) L'apport du principe constitutionnel d'impartialité et d'objectivité des fonctionnaires

Le principe constitutionnel d'impartialité et d'objectivité des fonctionnaires dans l'exercice de leurs missions de service public peut, quant à lui, constituer un apport adéquat pour former un cadre juridique général des investigations administratives numériques. Ce principe est d'ailleurs visé par l'Ombudsman dans la décision qui a servi de point de départ à la présente analyse. Celui-ci indique en effet que « la commission [municipale chargée des affaires sociales] doit, comme tout autre représentant de l'État, […] respecter les principes d'objectivité et d'impartialité dans l'exercice de sa mission, en vertu du chapitre 1, article 9 de l'Instrument de gouvernement »[14]. On peut regretter cependant que l'Ombudsman se soit contenté de citer le principe tel qu'énoncé dans le texte constitutionnel, sans en faire – comme il en a coutume – ressortir spécifiquement les éléments constitutifs tout particulièrement pertinents au regard de la décision en question, ou encore sans les rattacher explicitement au dit principe. En effet, le principe d'objectivité qui, dans son acception originelle, exprimait une obligation de conformité de l'action de l'administration à la loi, hors de toute considération subjective, a fait montre d'une formidable élasticité au fur et à mesure de la jurisprudence de l'Ombudsman, et présente désormais des éléments qui pourraient être tout particulièrement utiles pour encadrer la collecte de données personnelles sur Internet et les réseaux sociaux dans le cadre d'investigations administratives. Il est vrai que l'Ombudsman a bien fait appel

[11] Prop 1979/80:1, Partie A., p. 400 et 562, cité dans la décision Facebook, p. 5.
[12] Décision p. 7.
[13] Décision p. 7.
[14] L'Instrument de gouvernement forme, avec trois autres textes, la Constitution suédoise.

dans la décision Facebook au principe de « nécessité » de l'action des agents, en indiquant que c'est seulement s'il existe une raison rendant indispensable un contrôle, comme le contrôle des informations fournies par l'administré concerné, qu'une recherche sur Internet devrait avoir lieu[15]. Il est vrai aussi que l'instance de contrôle suédoise a souligné que la recherche d'informations doit avoir un « but précis » et que « l'information versée au dossier doit, comme tout autre information, avoir une importance pour le traitement de l'affaire »[16]. Cependant l'Ombudsman a manqué de présenter ces différentes règles sous l'angle du principe constitutionnel d'objectivité, ce qui, selon nous, aurait donné plus de poids à l'argumentation juridique développée.

Il nous semble regrettable d'autre part que l'Ombudsman n'ait pas puisé plus avant dans les ressources argumentatives fournies par le principe d'objectivité. Ainsi, pour ne citer que cet aspect[17], il aurait pu mettre en avant, comme il l'a fait dans des décisions antérieures, que le respect du principe d'objectivité par les agents ne se mesure pas seulement à l'aune de ce que le fonctionnaire considère être « objectif », mais également à l'aune de la perception qu'en ont les administrés concernés. Ainsi, par exemple, dans une décision concernant des communications mises en ligne sur un compte Facebook de la Police[18], l'Ombudsman avait critiqué la formulation de certaines d'entre elles pour leur tonalité inadéquate. En l'occurrence, bien que l'agent de police auteur des propos considérait ceux-ci comme anodins, l'Ombudsman a retenu une violation du principe d'objectivité dans la mesure où des internautes avaient perçu les messages en question comme inappropriés. D'ailleurs, comme le précise l'Ombudsman dans cette même décision, « l'existence même du risque que des tiers puissent sentir que les principes d'objectivité et d'impartialité ne sont pas respectés suffit pour que l'action des agents soit considérée comme non conforme aux exigences constitutionnelles ». Une référence à cette composante du principe d'objectivité aurait été la bienvenue, nous semble-t-il, dans le contexte des recherches des investigations administratives. Elle enjoindrait aux fonctionnaires de se poser la question du ressenti des administrés, notamment en termes de violation de leur vie privée, et poserait par conséquent des limites à leurs actions.

Par ailleurs, l'Ombudsman n'a-t-il pas manqué une opportunité d'enrichir et d'affiner le concept d'objectivité, comme il l'a fait au gré de sa jurisprudence antérieure, en y apportant de nouveaux éléments permettant de saisir la réalité de l'action administrative en pleine mutation technologique et sociétale ? Plus précisément, il nous semble que l'Ombudsman aurait pu judicieusement étoffer

[15] Décision Facebook, p. 7.
[16] Décision Facebook, p. 7.
[17] On pourrait citer également l'obligation, qui se dégage de ce principe, concernant *la qualité de l'information* traitée par l'administration ainsi que celle de faire usage d'une *information objective*.
[18] Décision nº 5875-2012, p. 7 et 8.

le principe d'objectivité, en s'y référant lorsqu'il a exprimé « que les services sociaux ne devraient pas s'adonner à des recherches sur Internet plus ou moins générales et systématiques d'informations concernant les demandeurs d'aide sociale »[19].

3) L'utilité de se référer au principe de protection de la vie privée

Le principe de la protection de la vie privée, auquel l'Ombudsman parlementaire ne s'est pas référé dans sa décision Facebook, pourrait également être utile à prendre en considération dans le façonnage d'un cadre juridique entourant la recherche et la collecte d'informations sur Internet et les réseaux sociaux, pratiques qui, par définition, engendrent un empiétement dans la sphère privée des personnes concernées. Pour ce qui est du droit suédois, trois pistes sont envisageables : l'obligation constitutionnelle faite aux autorités étatiques de respecter la vie privée des citoyens ; la prohibition constitutionnelle de surveiller et cartographier/profiler les individus et, enfin, l'obligation de respecter la vie privée introduite par l'incorporation, au moyen d'une loi, de la Convention européenne des droits de l'homme dans le droit suédois.

Premièrement, il serait loisible, pour protéger la vie privée des administrés face aux pratiques d'investigations administratives numériques, de faire usage de l'article 2 figurant au chapitre premier de l'Instrument de gouvernement qui pose les grandes lignes directrices des activités et des buts des pouvoirs publics. Cette disposition prévoit que les pouvoirs publics « doivent préserver la vie privée des individus ». Il ne s'agit pas d'une obligation justiciable, car ne faisant pas partie du catalogue des droits de l'homme consigné au second chapitre, mais l'Ombudsman y a parfois fait référence pour apprécier les actions des fonctionnaires. Par exemple, dans une décision de 2010[20] qui concernait la publication, sur le site officiel d'une municipalité, d'informations erronées relatives à un administré, l'Ombudsman avait rappelé l'obligation des autorités publiques de respecter la vie privée des individus prévue à l'article 2 du chapitre premier de l'Instrument de gouvernement, et avait critiqué en conséquence les agissements de la municipalité incriminée[21]. D'ailleurs, si cet article 2 pose principalement des obligations à caractère positif, c'est-à-dire requiert de l'État de « protéger, promouvoir et dans la plus grande mesure possible faire en sorte que le droit [en question] puisse être mis en œuvre »[22], cette disposition contient également « par nature » […] « une renonciation [des pouvoirs publics] à s'ingérer indûment dans le droit en question ». Cette dernière interprétation des obligations négatives des autorités de

[19] Décision Facebook, p. 7.
[20] Décision nº 4935-2009 du 16 février 2010.
[21] *Ibid.*
[22] Voir SOU 1975:75 Medborgerliga fri- och rättigheter, p. 184. Voir aussi *Integritets skyddet i regeringsformen,* Elisabeth Reimers, SvJT, 2009.

l'État, tirée des travaux préparatoires, devrait pouvoir s'appliquer aux situations telle que celle qui se présente dans l'affaire Facebook, afin de constituer un frein aux ingérences indues dans la sphère privée des administrés.

Une seconde disposition constitutionnelle en rapport avec la protection de la vie privée, justiciable cette fois car faisant partie du catalogue des droits fondamentaux, pourrait être potentiellement applicable aux opérations de recherche et de collecte d'informations personnelles sur Internet et les réseaux sociaux. Il s'agit de l'article 6, alinéa 2, du Chapitre 2 de l'Instrument de gouvernement – introduit lors de la réforme constitutionnelle de 2011 – qui prévoit une protection des citoyens contre « les ingérences notoires dans leur vie privée [effectuées par les organes publics] lorsque ces ingérences ne font pas l'objet d'un consentement et conduisent à la surveillance ou à la cartographie de la situation personnelle des individus concernés ». S'il est encore trop tôt pour se prononcer de façon tranchée sur l'applicabilité de cet article pour encadrer la pratique des investigations administratives dans le Cyberespace, certains indices de la jurisprudence balbutiante de l'Ombudsman amènent à penser que cette disposition peut avoir un rôle à jouer en la matière[23]. La réponse à la question dépend en grande partie de l'interprétation qui est et sera donnée aux termes de « cartographie » et de « surveillance », tels qu'employés par l'Instrument de gouvernement.

Outre les dispositions constitutionnelles susmentionnées, le dispositif de protection de la vie privée de la Convention européenne des droits de l'homme (CEDH) peut également être pressenti pour protéger des atteintes causées par les investigations administratives numériques. La Convention, qui a été incorporée dans le droit suédois par la loi (1994 : 1219) sur la Convention européenne[24] entrée en vigueur le 1er janvier 1995, fait en effet partie intégrante du droit positif suédois[25].

D'ailleurs, le texte de la Convention européenne qui, de ce fait, peut être invoquée devant les instances nationales en tant que droit national positif, bénéficie en outre d'un statut particulier puisqu'une disposition constitutionnelle interdit au législateur de légiférer d'une manière incompatible avec la CEDH[26]. L'incorporation de la CEDH dans le droit suédois a conduit à deux apports d'importance en ce qui concerne les garanties entourant le droit au respect de la vie privée. Premièrement, le mode de protection est renforcé puisque, tandis que le chapitre 2 de l'Instrument de gouvernement prévoit la protection contre les

[23] Comme dans la décision sur l'utilisation de méthodes policières d'investigation non conventionnelles, voir note 32.

[24] En effet, l'État suédois, d'inspiration dualiste, a pris la décision, au moment de son entrée dans l'Union européenne, d'incorporer la Convention dans son droit, à l'instar du Danemark et de la Finlande d'approche également dualiste.

[25] Nous analyserons plus en détail, lors de l'examen du droit européen, les dispositifs protecteurs émanant de cette disposition et nous nous contenterons ici de dire quelques mots des rapports de la Convention et du droit suédois.

[26] Chapitre 2, Article 19 de l'Instrument de gouvernement.

seules atteintes portées aux individus (par l'État), c'est-à-dire des obligations qualifiées de négatives, l'article 8 de la CEDH emporte aussi bien des obligations négatives que positives[27]. Deuxièmement, l'objet de la protection se trouve élargi par rapport à celui émanant du chapitre 2 de l'Instrument de gouvernement. En effet, tandis que l'instrument juridique suédois ne protège, au titre des droits fondamentaux, que certains aspects de la vie privée (protection du domicile[28], des correspondances[29], protection contre la cartographie[30], etc.), l'article 8 de la CEDH prévoit une protection de la vie privée en général. L'Ombudsman a d'ailleurs su tirer profit de cet élargissement du champ de protection de la vie privée. Ainsi, dans une décision relative à l'utilisation par les autorités policières suédoises de méthodes non conventionnelles pour recueillir de la part d'un suspect des aveux de son implication dans des actes de nature criminelle[31], l'instance suédoise a eu recours à l'article 8 de la CEDH et à la jurisprudence afférente de la Cour de Strasbourg afin de démontrer le caractère illégal des agissements de la Police[32]. Cet exemple illustre, à notre sens, la potentialité de l'utilisation de l'article 8 de la CEDH par l'Ombudsman parlementaire pour protéger les administrés contre les atteintes à leur vie privée engendrées par la recherche et la collecte d'informations personnelles sur Internet et les réseaux sociaux. La référence à une telle base légale sera d'autant plus opportune s'il s'avère que le nouvel article 6.2 du chapitre 2 de l'Instrument de gouvernement, qui garantit les individus contre les atteintes liées à la surveillance et la cartographie[33], se révèle inefficace pour encadrer les pratiques d'investigations administratives effectuées à l'aide d'outils (moteurs de recherche) et de plateformes numériques.

Les principes examinés ci-dessus – d'objectivité et de protection de la vie privée – peuvent constituer, tout au moins entre les mains de l'Ombudsman parlementaire, pierre angulaire du contrôle du respect de la loi et des principes de bonne administration par les autorités publiques[34], un référentiel légal opératoire pour encadrer de façon générale les investigations

---

[27] Voir, par exemple, Hans Danelius, Mänskliga rättigheter i europeisk praxis – En kommentar till Europakonventionen om de mänskliga rättigheterna, Norstedts Jurdik, 2012, p. 347.

[28] Instrument de gouvernement, Chapitre 2, Article 6, 1er alinéa.

[29] Instrument de gouvernement, Chapitre 2, Article 6, 1er alinéa.

[30] Instrument de gouvernement, Chapitre 2, Article 6, alinéa 2.

[31] Décision nº 0731-2010 et 3652-2010 du 28 novembre 2011.

[32] L'instance de contrôle suédoise ne pouvait s'appuyer en l'occurrence sur l'article 6.2 du Chapitre 2 de l'Instrument de gouvernement garantissant la protection des citoyens « *contre des atteintes significatives à leur vie privée survenant en dehors de leur consentement et aboutissant à la surveillance ou à la cartographie de leur situation personnelle* ». En effet, bien qu'entrée en vigueur au moment du rendu de la décision, elle ne l'était pas au moment de la commission des agissements policiers incriminés. L'Ombudsman avait toutefois visé cette nouvelle disposition.

[33] Voir *supra*.

[34] Voir P. JONASON, « L'Ombudsman suédois, un protecteur des droits fondamentaux qui se découvre », *Revue Droit, Société et Pouvoir*, 2017, nº 6, Laboratoire de Recherche Université d'Oran, pp. 210-221.

administratives sur le Cyberespace. Au-delà des règles nationales, des règles d'origine européenne apportent un cadre non négligeable et même irréfragable pour ce genre d'investigations.

B) Le cadre d'origine européenne

Voyons quel cadre la législation de l'Union européenne sur la protection des données personnelles (1) et l'article 8 de la Convention européenne des droits de l'homme (2) fournissent aux investigations administratives opérées au moyen de la collecte d'informations personnelles sur Internet et les réseaux sociaux.

1) La législation européenne sur la protection des données à caractère personnel

Les investigations administratives sur Internet et les réseaux sociaux sont soumises, dans la partie qui relève de la collecte et de l'utilisation ultérieure des données glanées sur les plateformes sociales et les moteurs de recherche, et en tant qu'elles correspondent à des traitements de données personnelles, aux règles de la législation européenne sur la protection des données personnelles. Ces règles, qui émanent plus précisément de la directive européenne sur la protection des données personnelles de 1995, bientôt remplacée par le règlement général sur la protection des données adopté en 2016[35] et dont l'entrée en vigueur est prévue pour mai 2018, sont tout particulièrement les Principes de légitimation des traitements (Directive)/Licéité du traitement (Règlement) d'une part, et les Principes relatifs à la qualité des données (Directive)/Principes relatifs au traitement des données à caractère personnel (Règlement).

Premièrement donc, le traitement effectué (la collecte, tout comme l'utilisation ultérieure des données) doit répondre aux conditions de légitimation du traitement (article 7 de la Directive)/de licéité du traitement (article 6 du Règlement). Il ne fait aucun doute que la collecte d'informations sur Internet et les réseaux sociaux dans le cadre d'investigations administratives peut être légitimée/être rendue licite en ce qu'un tel traitement « est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (article 7-e de la Directive et article 6-e du Règlement).

En second lieu, il découle des dispositifs susmentionnés que l'administration qui collecte des informations personnelles sur Internet et les réseaux sociaux a l'obligation de respecter les principes de licéité, de loyauté, de transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la conservation des données, ainsi que les principes d'intégrité

[35] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

et de confidentialité, et enfin le principe de responsabilité (article 6 de la Directive et article 5 du Règlement). Parmi ces obligations, sans doute celle de la transparence du traitement à l'égard de la personne concernée est-elle la plus révélatrice des problèmes que pose la collecte de données dans le cadre d'investigations administratives sur Internet. Ainsi, dans l'affaire traitée par l'Ombudsman parlementaire suédois, la collecte d'informations sur le compte Facebook de la plaignante et sur le blog de l'une de ses amies avait eu lieu à l'insu de l'administrée. Il est intéressant de noter toutefois que, en ce qui concerne les traitements nécessaires à l'exécution d'une mission d'intérêt public, le Règlement laisse aux États membres une marge de manœuvre dans l'énoncé des règles. Ces derniers pourront en effet « maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement […] en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal […] » (article 6.2). Le législateur national aura ainsi tout le loisir de prévoir des exigences permettant de prendre en compte la particularité de la collecte d'informations sur Internet et les réseaux sociaux.

Ajoutons enfin que le Règlement (article 6.3) précise que de tels traitements doivent être fondés sur le droit de l'Union ou d'un État membre auquel le responsable de traitement est soumis, et que la base juridique du traitement « peut contenir des dispositions [sur le type de données traitées, les limitations des finalités, etc.] spécifiques pour adapter l'application des règles du présent règlement ». Quoi qu'il en soit, la liberté des États membres sur ce point est encadrée. Le règlement précise en effet que « le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. » (article 6.3 in fine du Règlement). Ceci n'est pas sans rappeler les termes de l'article 8 de la CEDH qui, garantissant le droit au respect de la vie privée, permet d'y apporter des limitations sous certaines conditions.

Comme on le voit, la législation de l'Union européenne sur la protection des données à caractère personnel exige que la collecte sur Internet et les réseaux sociaux de données personnelles et l'utilisation ultérieure de ces données soient encadrées par le droit. Quoi qu'il en soit, cette législation ne rend pas compte de toutes les dimensions inhérentes aux pratiques administratives consistant à rechercher, collecter et utiliser des informations publiées sur Internet et les réseaux sociaux, dans le cadre de leurs investigations. En effet, l'ingérence dans la vie privée ne se confine pas à celle causée par la collecte des informations et leur utilisation dans la gestion du dossier administratif. Elle est plus largement liée à la manière dont les investigations elles-mêmes sont pratiquées et au sentiment d'être surveillé et épié qu'elles engendrent chez les administrés. Autrement dit, au-delà des règles protectrices des données personnelles, il convient de s'intéresser aux règles protectrices de la vie privée, et plus particulièrement à

l'article 8 de la Convention européenne sur les droits de l'homme[36].

2) L'article 8 de la Convention européenne des droits de l'homme et la protection de la vie privée

L'article 8 de la CEDH, qui met à la charge des États des obligations négatives ainsi que des obligations positives en matière de protection de la vie privée, et qui part d'une définition de la vie privée aux larges contours, devrait pouvoir s'appliquer sans difficulté à la situation décrite dans la présente analyse.
Certes, il n'existe pas encore de décision relative à la recherche, la collecte et l'utilisation par les administrations d'informations personnelles collectées sur Internet, et notamment sur les réseaux sociaux, dans le cadre d'investigations administratives à proprement parler. En outre, il est vrai que la plupart des affaires soumises à la Cour européenne des droits de l'homme, qui mettent en lumière la problématique de la surveillance et de la cartographie des citoyens réalisées par les autorités publiques concernent le domaine des investigations effectuées par la police ou l'armée dans le but de protéger la sécurité nationale[37]. Cependant, une décision du 18 octobre 2016, *Vukota-Bojić c. Suisse*[38] dans laquelle la Cour de Strasbourg a condamné l'État helvétique pour des activités de surveillance attentatoires à la vie privée effectuées à l'encontre d'une assurée par une compagnie d'assurance à caractère public, constitue – moins d'ailleurs pour les procédés employés pour effectuer la surveillance que pour les buts de celle-ci – un premier précédent à l'aune duquel peut être

---

[36] Rappelons que la Charte des droits fondamentaux de l'Union européenne, que le Traité de Lisbonne a rendu juridiquement contraignante, comporte une disposition protégeant la vie privée (article 7) et une autre consacrée tout particulièrement à la question de la protection des données (article 8). Notons également qu'il existe une inspiration réciproque entre les deux branches du droit européen sur la question de la vie privée/protection des données personnelles. Voir sur ce point par exemple M. MCDONAGH, *Balancing Disclosure of Information and the Right for Private Life in Europe*, pp. 3-4: https://www.researchgate.net/publication/281436645_Balancing_Disclosure_of_Information_and_the_Right_to_Respect_for_Private_Life_in_Europe

[37] Ainsi, dans l'arrêt Murray contre Royaume Uni de 1994 (requête n°14310/88), la Cour s'était prononcée sur la plainte d'une requérante qui avait mis en cause des agents (militaires) qui avaient procédé à la consignation de détails personnels la concernant, elle et sa famille, et avait pris une photo d'elle à son insu ou sans son consentement. Tenant compte de ce que la requérante était possiblement impliquée dans une affaire de traffic d'armes pour le compte de l'IRA, la Cour avait cependant conclu que l'atteinte à la vie privée invoquée était légitimée en tant que conforme aux conditions posées par le second paragraphe de l'article 8. Plus récemment, dans l'arrêt *Szabó et Vissy contre la Hongrie* du 12 janvier 2016 (requête 37138/14) la Cour de Strasbourg a condamné le pays défendeur pour violation de l'article 8 de la CEDH, au motif que les modifications apportées à la législation hongroise pour lutter contre le terrorisme (avec notamment la création d'une Task Force spéciale) et attaquées par les plaignants n'étaient pas suffisamment détaillées et n'offraient pas de garanties suffisantes contre les abus et l'arbitraire. Un autre exemple est fourni par l'affaire pendante *Tretter and Others v. Austria* (requête n° 3599/10) concernant des amendements apportés à la loi sur les pouvoirs de police, entrés en vigueur en janvier 2008, élargissant le pouvoir des autorités policières de collecter et traiter des données personnelles.

[38] Requête n° 61838/10.

discutée la validité de notre hypothèse.

L'affaire est la suivante : la requérante, qui avait été victime en 1995 d'un accident de la route, avait obtenu de son assurance le versement d'une pension d'invalidité. Après avoir en 1997 passé des examens médicaux qui avaient conclu au recouvrement total des facultés de travail de la requérante, puis une batterie de tests qui attestaient au contraire l'existence d'un handicap, et après plusieurs années de contentieux, l'assureur demanda à la requérante de se soumettre à un nouvel examen médical. Face au refus opposé par cette dernière, l'assureur engagea des détectives privés pour suivre les déplacements de la requérante et réunir des preuves sur son état de santé. Les actes de surveillance ont consisté en pratique à ce que les détectives ont, sur une période de trente-trois jours, à quatre reprises et sur de longues distances, suivi et filmé Mme Vukota-Bojić dans des lieux publics et ont établi des rapports de leurs observations. Les preuves recueillies ont été utilisées à charge lors d'un procès contre la requérante et mises à profit pour obtenir du tribunal une diminution conséquente de la pension d'invalidité de celle-ci. Devant la Cour de Strasbourg, Mme Vukota-Bojić a eu gain de cause sur la question des allégations de violation du respect de la vie privée mais n'a pas été suivie en revanche en ce qui concerne le grief de violation de son droit à un procès équitable en matière civile qu'elle avait également invoqué.

Sur le terrain de l'Article 8, la Cour a considéré que la surveillance exercée à l'égard de la requérante, caractérisée par un caractère permanent des images, ainsi que l'utilisation de celles-ci dans le cadre du règlement d'un litige d'assurance peuvent être regardées comme un traitement ou une collecte de données personnelles concernant la requérante « révélant une ingérence dans sa "vie privée" au sens de l'article 8 § 1 »[39].

Pour en arriver à cette conclusion relative à l'application de l'Article 8-1, la Cour a notamment fait valoir que « la notion de" vie privée" au sens de l'article 8 est une notion large, qui ne se prête pas à une définition exhaustive » et qui « protège entre autres le droit à l'identité et au développement personnel, ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur ». La Cour poursuit en disant qu' « existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée »[40]. Le juge européen a également pris en considération des circonstances telles que celles de savoir « si des informations avaient été recueillies sur une personne bien précise, si des données à caractère personnel avaient été traitées ou utilisées et si les éléments en question avaient été rendus publics d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre »[41].

[39] Point 59.
[40] Point 52.
[41] Point 56.

Une telle acception de la vie privée, qui va au-delà du cercle purement privé et insiste sur la fonction sociale de ce droit, semble bien calquer la situation des investigations administratives sur Internet et les réseaux sociaux qui, de facto, portent sur des interactions entre internautes. Un élément d'appréciation de l'atteinte à la vie privée, qui pourrait par contre faire défaut, est celui qui tient compte de « ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée »[42]. En effet, on peut se demander à quel seuil de respect de sa vie privée s'attend un internaute/facebooker alors qu'il expose de façon plus ou moins maîtrisée sa vie privée sur le Cyberespace. L'argument qui consiste à dire que les utilisateurs de réseaux sociaux doivent s'en prendre à eux-mêmes si l'administration récolte des données sur lesdits réseaux, et ne pourraient par conséquent invoquer une ingérence dans leur vie privée – argument qui a été employé par l'Ombudsman dans la décision suédoise étudiée[43] – est toutefois réfutable à plusieurs points de vue. Premièrement « l'attente raisonnable » si elle « peut constituer un facteur important » pour la Cour, dans l'appréciation de l'ingérence, n'est cependant d'après cette même Cour « pas nécessairement décisive »[44].

Deuxièmement, dans le cadre de sa recherche d'éléments potentiellement intéressants pour le traitement du dossier dont il est chargé, l'agent de l'administration aura certainement un champ de ratissage plus large que les seules pages Facebook de l'administré en question. Il sera ainsi sans doute amené à glaner des informations en provenance de sources dont l'intéressé n'a pas le contrôle. Dans notre affaire suédoise, les services sociaux avaient ainsi récolté des informations sur le blog d'une amie de la plaignante.

On pourra arguer sans doute que la surveillance, telle qu'effectuée dans le cas suisse à l'aide d'une caméra, est d'un autre calibre que la surveillance effectuée sur Internet et les réseaux sociaux. S'il y a incontestablement une différence dans la brutalité et l'intensité des méthodes employées, le caractère insidieux et rampant des investigations du type Facebook est lui aussi problématique. Quoi qu'il en soit, dans les deux cas, l'administration, qui a agit sous visage couvert, a accumulé des éléments permettant la vérification des dires d'un citoyen dans le cadre du traitement de son dossier. Et le résultat des investigations est le même : l'intéressée s'est sentie, dans un cas comme dans l'autre, épiée et visée dans son

[42] Point 54.

[43] L'Ombudsman auteur de la décision Facebook fait en effet référence, en en approuvant les conclusions, à une décision du 16 octobre 2008 prise par un autre Ombudsman dans une affaire dans laquelle une caisse de sécurité sociale avait récolté des informations sur le blog d'un assuré social, dans le cadre du traitement de son dossier. L'Ombudsman n'avait alors pas émis de critique à l'égard de la caisse de sécurité sociale mise en cause, au motif qu'une personne qui publie des informations de la sorte doit tenir compte de ce que celles-ci sont également accessibles aux autorités publiques, et que ces dernières ont l'obligation de prendre en considération toutes les informations qui arrivent à leur connaissance.

[44] Point 54.

intégrité[45].

Malgré des dissimilitudes concernant notamment le modus operandi, il nous semble donc qu'il soit possible de s'appuyer sur l'arrêt *Vukota-Bojić* pour considérer que – dans certains cas au moins – la recherche, la collecte et l'utilisation de données personnelles, dans le cadre d'investigations administratives numériques, répondent aux critères posés par l'article 8.1 sur l'existence d'une ingérence dans la vie privée.

Qu'en est-il de la question de la justification de l'ingérence ? Autrement dit, une telle ingérence est-elle prévue par la loi en vertu de l'article 8.2, au sens où l'entend la CtEDH ? Dans l'affaire *Vukota-Bojić c. Suisse*, la Cour, ayant passé en revue les textes nationaux en vigueur, admet que les dispositions légales pertinentes, lues ensemble, permettent aux autorités suisses d'assurance, en cas de réticence de l'assuré à fournir les informations demandées, de prendre les mesures d'investigation appropriées et de collecter les informations nécessaires. La Cour a convenu également que les dispositions en question étaient « accessibles » à l'intéressée[46]. En revanche, le juge européen blâme le dispositif suisse au motif qu'il n'offre pas de garanties suffisantes contre les abus[47], et qu'il est, de plus, muet sur les procédures de stockage, d'accès, d'examen, d'utilisation, de communication et de destruction des données collectées à l'aide de mesures de surveillance secrètes[48]. Par conséquent, la Cour conclut à une violation de l'article 8, sans avoir à se prononcer sur la question de savoir si les mesures attaquées étaient « nécessaires dans une société démocratique ».

Les exigences posées par cet arrêt, quant aux conditions de rigueur légale, devant entourer la procédure de surveillance mise en œuvre, devraient pouvoir s'appliquer à la recherche et la collecte d'informations personnelles sur Internet et les réseaux sociaux dans le cadre d'investigations telles qu'effectuées dans l'affaire Facebook.

Il ressort de l'examen des textes qui précède que la mise en conformité des investigations administratives numériques au droit européen suppose, en tant que celles-ci conduisent à la mise en œuvre de traitements de données personnelles et à de potentielles ingérences au droit à la vie privée, l'adoption de textes prévoyant les conditions de traitements de données personnelles ainsi que des mécanismes permettant d'éviter les abus et l'arbitraire[49].

---

[45] On peut relever une différence notoire toutefois entre les deux affaires : tandis que les informations documentées ont été utilisées dans le cas suisse à l'appui de la décision de diminuer la pension d'invalidité, celles recueillies sur Internet dans le cas suédois n'ont pas été prises en compte dans la décision prise par les services sociaux.

[46] Point 70.

[47] Points 73 et 74.

[48] Point 75.

[49] Nous émettons un doute sur la conformité du droit suédois actuel à ces exigences. Une solution envisageable pour remédier à cette situation pourrait être l'introduction dans la loi sur la procédure administrative, actuellement objet d'une réforme, d'une disposition qui porterait sur les méthodes d'investigation administratives et poserait

Quoi qu'il en soit, si un texte clair, accessible et contenant des mécanismes de protection est indispensable, il nous semble, qu'au regard de l'importance et de la pluralité des enjeux en présence dans le cadre des investigations administratives telles qu'ici étudiées, de tels dispositifs à caractère contraignant doivent être accompagnés d'instruments relevant de la *soft law*.

§ 2 – UN CADRE JURIDIQUE EN PARTIE SOUPLE

La question de la régulation des pratiques administratives de recherche et de collecte des données sur les réseaux sociaux, et plus généralement sur Internet, est complexe. Il s'agit de concilier l'efficacité administrative avec deux impératifs primordiaux : la protection de la vie privée et, au-delà, la protection des fondements de la démocratie (A). Or, un texte contraignant, s'il semble nécessaire pour les raisons susmentionnées, n'en est pas pour autant suffisant pour appréhender les différentes dimensions impliquées par ces méthodes. En effet, un tel texte ne peut avoir qu'un caractère général et assez vague, tandis que la mise en œuvre d'investigations administratives numériques requiert une appréciation au cas par cas des limitations pouvant être légitimement apportées aux libertés des administrés. Ceci implique la mise à la disposition des fonctionnaires d'un manuel les guidant dans la prise de décision concernant les investigations administratives au moyen d'Internet et des réseaux sociaux (B).

A) Les enjeux multiples liés aux pratiques administratives d'investigation sur Internet

L'utilisation des plateformes (réseaux sociaux ou autres) et d'outils (tels les moteurs de recherche) fournis par Internet n'est pas anodine du point de vue des droits et libertés fondamentaux des individus, et au-delà, des fondements d'une société démocratique.

Premièrement, cette méthode a de nombreuses implications dans le domaine de la protection de la vie privée. Les quatre composantes que nous incluons dans cette notion[50] – le « droit d'être laissé en paix » (*the right to be let alone*), le droit à l'autodétermination informationnelle, le « pouvoir d'une personne de se comporter comme elle l'entend dans cette partie de sa vie »[51] et la possibilité de l'individu de participer à la vie en société – sont toutes impactées par les méthodes d'investigation administratives. Loin d'être *laissées en paix* par les pouvoirs publics, les personnes

l'obligation de respecter certains principes en ce qui concerne la recherche et la collecte de données.

[50] Il existe une pléthore de définitions de la notion de vie privée. Nous en retenons la définition présente, qui comporte quatre facettes, Voir P. BLANC-GONNET JONASON, « Démocratie, transparences et État de droit – la transparence dans tous ses états », *European Review of Public Law*, vol. 27, nº 1, 2015, pp. 122-124.

[51] In *La protection de la vie privée par le droit*, Economica, 3e éd. 1995, pp. 11 et 12. M. Kayser souligne que J. RAVANAS a traité de cette distinction in : Protection de la vie privée, *Jurisclasseur*, Jouissance des droits civils, art. 9, Fasc. 1, nº 5, 20 et s.

soumises à ce genre d'investigation se sentent épiées par les agents de l'administration. Le cas suédois Facebook en témoigne. En outre, ces pratiques mettent au jour *la perte de contrôle* des citoyens sur l'utilisation qui est faite de leurs données et sur le façonnement de leur propre image. En effet, l'administration utilise des informations/données qui ne leur sont pas destinées, qui plus est, à l'insu des personnes concernées. En outre, le recours aux possibilités offertes par les moteurs de recherche est susceptible d'entraîner deux types de risques particuliers à l'égard de la vie privée de la personne concernée. Il s'agit, premièrement, du danger d'agrégation[52] qui provient de la possibilité de cartographier une personne visée, grâce à la masse d'informations obtenue sur cette personne à l'aide de moteurs de recherche. Le second danger, celui de distorsion[53], consiste, quant à lui, en ce que les informations collectées mises bout à bout ne donnent pas forcément une image fidèle de la personne concernée, soit qu'il manque des pièces importantes du puzzle de sa vie, soit que certains aspects soient trop ou trop peu mis en évidence, soit encore que des éléments non conformes à la réalité personnelle de l'intéressé soient présentés comme vérité.

Il n'est pas difficile de concevoir que les composantes du droit à la vie privée consistant dans le « pouvoir d'une personne de se comporter comme elle l'entend dans cette partie de sa vie » ainsi que la « possibilité de l'individu de participer à la vie en société » sont elles aussi mises à mal lorsque les administrations effectuent des contrôles à partir des réseaux sociaux. Le rôle principal de ces plateformes est en effet, pour les individus, de servir de vitrine à l'adresse de leurs semblables, de leurs activités et de leurs choix de vie. Les réseaux sociaux constituent des outils d'action et d'interaction sociétales par excellence.

Les risques causés par les investigations administratives sur Internet ne se confinent pas à des ingérences dans la vie privée de la personne directement concernée par l'enquête administrative mise en cause, mais peuvent avoir des répercussions plus larges. En effet, le droit au respect de la vie privée n'a pas uniquement une valeur individuelle de protection des personnes concernées mais a également une valeur collective de protection de la société et des valeurs démocratiques dans leur ensemble. La reconnaissance de la valeur sociétale du respect de la vie privée, que l'on trouve dans la célèbre décision *census* de 1983 du Tribunal fédéral constitutionnel allemand[54], se retrouve également chez le juge européen. Ainsi, dans son arrêt *Digital Rights*[55] par lequel elle a invalidé la directive 2006/24/CEE du15 mars 2006 sur la

[52] Voir D. J. SOLOVE, "Nothing to hide" – *The False Tradeoff between Privacy and Security*, Yale University Press, 2011, p. 27.
[53] *Id.*, p. 28.
[54] Voir la décision du 15 décembre 1983, BVerfG, *EUGRZ*, 1983, 588, dans laquelle le Tribunal de Karlsruhe exprime que la capacité d'autodétermination des individus, outre qu'elle est une condition nécessaire au développement individuel, constitue une condition essentielle à la vie démocratique.
[55] Arrêt du 8 avril 201, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd, Kärntner Landesregierung.*

conservation de données pour non-conformité aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, la Grande Chambre de la CJUE souligne explicitement le risque que fait peser sur la liberté d'expression des citoyens la conservation des données de communication par les opérateurs[56]. D'après la Cour, en effet, « *il n'est pas exclu que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive, et en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte* ». Cette prise de conscience a désormais un écho en Suède : dans un rapport parlementaire intitulé « Comment se porte la vie privée ? »[57], les rapporteurs, sous une rubrique à l'intitulé révélateur « La vie privée, une valeur d'importance pour la société tout entière »[58], font valoir que le droit à la vie privée est « un élément important également pour [… les] droits et libertés fondamentaux qui constituent la base d'une société démocratique, et en particulier la liberté d'expression, le droit à l'information et le droit de communication »[59]. Et le rapport poursuit « […] des valeurs fondamentales peuvent être menacées si les individus renoncent à entreprendre des activités à cause d'une perte de confiance ou de la crainte d'être enregistrés, cartographiés ou bien surveillés d'une manière qui à terme pourraient leur porter préjudice »[60].

Il ne fait pas de doute que l'utilisation par l'administration de méthodes d'investigation à partir d'informations personnelles glanées sur Internet et les réseaux sociaux puisse entraîner une réaction d'autocensure et plus généralement d'autolimitation chez les citoyens. Celle-ci peut se traduire par un frein des internautes à la publication d'informations sur leurs propres comptes de réseaux sociaux. L'autolimitation peut se traduire également – ce qui peut constituer une atteinte encore plus grave à la liberté des personnes – en la réticence des citoyens à prendre part à des activités qui laisseront des traces sur Internet, comme celle de participer à une manifestation sportive ou à un colloque, par exemple, ou encore d'adhérer à une association. De façon concomitante, il existe le risque que ne se délite la confiance des citoyens dans l'État et dans le professionnalisme de ses agents. Avoir affaire à un agent public qui connaît tout de soi n'est pas propice à l'instauration d'un climat de confiance.

B) Les apports d'un texte juridique souple

Face à ces enjeux, tant multiples que primordiaux, un texte à valeur contraignante encadrant les investigations administratives numériques ne saurait suffire, surtout s'il s'agit d'un texte général (c'est-à-dire non sectoriel) au caractère forcément vague. En effet,

[56] Point 28.
[57] Hur står det till med den personliga integriteten, SOU 2016 :41.
[58] « Personlig integritet ett viktigt värde för hela samhället »
[59] SOU 2016 : 41, p. 61.
[60] *Id.*

les fonctionnaires ont besoin d'une boussole relativement précise les aidant, au cas par cas, à apprécier la légalité et la légitimité d'un recours aux investigations à l'aide d'Internet.

On peut imaginer que le texte contraignant exigé par le droit européen pose le principe de l'interdiction, pour les autorités publiques, de glaner sur Internet des informations sur les administrés, à moins que la recherche d'informations soit nécessaire dans le cadre du traitement d'un dossier administratif particulier, et que l'atteinte au droit au respect de la vie privée, potentiellement causée par les investigations, soit proportionnée au but recherché. Ce texte contraignant pourrait également imposer à l'administration le respect des principes de protection des données personnelles pour les informations à caractère personnel collectées sur Internet (à moins que de telles règles ne soient consignées dans un texte plus général relatif aux traitements de données personnelles effectués par l'administration).

Il appartiendra au texte ayant la nature de soft law de fournir la liste des facteurs dont les fonctionnaires devront tenir compte pour apprécier le juste équilibre entre les intérêts en présence. Au nombre de ceux-ci, la question de l'ingérence dans la vie privée des administrés susceptibles d'être soumis à de telles pratiques et, au-delà, celle des risques pour les valeurs démocratiques engendrés par ces mêmes pratiques, arrivent en bonne position. Autrement dit, outre son aspect d'aide à la décision, cet instrument au caractère souple devrait avoir une tonalité pédagogique renforcée, dans le but de faire prendre conscience aux fonctionnaires des enjeux de leurs actes.

Ce texte devra en outre, sous la forme de lignes directrices, expliciter plus avant les éléments dont le fonctionnaire doit tenir compte pour réaliser l'équilibre susmentionné[61]. Parmi les questions que devra se poser le fonctionnaire en charge des investigations on peut citer les suivantes[62] : quelles sont les informations dont disposent déjà le fonctionnaire ? Quel est le besoin d'obtenir des informations supplémentaires ? Quel est l'enjeu pour l'administration de se procurer les informations manquantes ? A-t-on incité l'administré à fournir les informations qui font défaut ? Y a-t-il des raisons de douter de la véracité des informations déjà disponibles ? A-t-on informé l'administré de ce que l'administration est susceptible de ratisser Internet (la transparence étant à préférer) ?

Le juste équilibre des intérêts en présence implique de la part des fonctionnaires une connaissance du contexte technologique,

[61] L'Ombudsman suédois dans sa décision Facebook aborde lui-même la question de la nécessité de l'existence de lignes directrices, en faisant notamment valoir qu'il ne devrait pas incomber au fonctionnaire seul de déterminer dans quels cas il est opportun de procéder à des recherches sur Internet dans le cadre des investigations administratives. L'Ombudsman cite, comme exemple à suivre et à développer, les lignes directrices adoptées par certaines administrations parmi lesquelles l'Agence Nationale des Affaires Sociales (Socialstyrelsen).

[62] Certains de ces éléments rejoignent d'ailleurs des points mis en exergue par l'Ombudsman suédois dans la décision Facebook.

informationnel et sociétal et également de l'impact de la recherche et de la collecte d'informations sur Internet et les réseaux sociaux sur la vie privée et les valeurs démocratiques. Parmi les éléments à rappeler aux fonctionnaires, et même si cela va de soi, pourraient figurer la large utilisation des réseaux sociaux dans la population[63], les buts premiers de l'utilisation de ces réseaux sociaux par les personnes privées, à savoir la communication entre pairs, mais aussi le fait que de nombreuses informations à caractère personnel que l'on trouve sur Internet sont publiées hors du contrôle des personnes concernées, voire à leur insu, et que la participation à des activités, même les plus anodines, comme par exemple l'affiliation à une association, la participation à un événement sportif ou scientifique laissent des traces sur le Cyberespace. Il serait bon d'indiquer aussi la nécessité pour le fonctionnaire de porter un regard critique sur les données accessibles et collectées, eu égard notamment aux risques de distorsion. Il convient de sensibiliser les agents de l'administration au fait que la recherche et la collecte des données sur les réseaux sociaux sont porteurs de risques pour la vie privée des individus et pour la démocratie, en informant de façon pédagogique des risques de perte de confiance dans l'État ainsi que des risques d'autolimitation de la liberté de se comporter et de communiquer comme on l'entend.

Enfin, il serait approprié de rappeler aux fonctionnaires leur devoir de professionnalisme. Il ne s'agit pas pour eux de céder à la curiosité ordinaire des internautes, stimulée notamment par l'accès à des photos. Le respect d'une déontologie en la matière étant indispensable pour la bonne relation entre l'administré et le fonctionnaire en charge de son dossier et, plus généralement, pour la confiance du public dans les représentants de l'État.

CONCLUSION

Il semble inévitable, et même dans une certaine mesure parfois louable, que les administrations mettent à profit les possibilités fournies par les nouvelles technologies, notamment les moteurs de recherche et les nouvelles plateformes sociales, pour contrôler les informations relatives aux administrés. L'aspect ordinaire de telles méthodes d'investigation administratives (en ce sens que les administrations font usage d'outils et de plateformes numériques mis à la disposition de tout individu lambda, et que, tout comme ce dernier, le fonctionnaire a acquis des réflexes d'efficacité « googlelisante » et est atteint de curiosité « facebookienne ») ne doit pas faire oublier le caractère potentiellement attentatoire de telles façons d'agir si elles ne sont pas adéquatement encadrées. Il est grand temps pour les législateurs nationaux de s'emparer de cette question afin d'éviter l'emprise insidieuse de ce nouveau Big Brother qui s'accompagne irrémédiablement du dévoiement du respect de la vie privée des citoyens, du délitement de la confiance

[63] Comme le font les lignes directrices de l'Agence Nationale des Affaires Sociales.

de ceux-ci à l'égard de leurs gouvernants et, au-delà, d'un affaiblissement de la démocratie.