Tracés. Revue de Sciences humaines

#19 | 2019
Les sciences humaines et sociales au travail (ii): Que faire des données de la recherche ?

Les chercheurs face à la surveillance d'État : état des lieux et contre-mesures

Researchers in the face of state surveillance: a critical overview and possible countermeasures

Félix Tréguer et Camille Noûs

Édition électronique
URL : http://journals.openedition.org/traces/11038
DOI : 10.4000/traces.11038
ISSN : 1963-1812

Éditeur
ENS Éditions

Édition imprimée
Date de publication : 31 décembre 2019
Pagination : 129-144
ISBN : 979-10-362-0227-8
ISSN : 1763-0061

Les chercheurs face à la surveillance d'État : état des lieux et contre-mesures

Researchers in the face of state surveillance: a critical overview and possible countermeasures

Félix Tréguer et Camille Noûs

> Le principe d'indépendance des enseignants-chercheurs n'implique pas que les professeurs d'université et maîtres de conférences doivent bénéficier d'une protection particulière en cas de mise en œuvre à leur égard de techniques de recueil de renseignement dans le cadre de la police administrative. Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015, § 36

1 Depuis les révélations de 2013 du lanceur d'alerte Edward Snowden sur les pratiques de surveillance des agences de renseignement occidentales, l'exposition du champ de la recherche en sciences sociales à la surveillance d'État – celle mise en œuvre par les appareils judiciaires et policiers, et plus largement justifiée par des impératifs de sécurité publique – a fait l'objet d'une attention croissante au niveau international (Tanczer *et al.*, 2016). Cette problématique s'inscrit dans une série d'enjeux plus larges touchant à une question essentielle et ancienne : celle de la préservation de l'autonomie du champ de la recherche face aux processus de managérialisation, de judiciarisation mais aussi de sécurisation qui traversent nos sociétés[1].

2 En France, la mise à l'agenda de ces enjeux intervient dans le contexte de la multiplication des procédures judiciaires et disciplinaires à l'encontre de chercheurs au cours des années 2000. Plusieurs affaires survenues à l'époque – la plus marquante étant sans doute l'affaire Vincent Geisser, du nom de ce chercheur spécialiste de l'islam harcelé par le fonctionnaire de sécurité de défense du CNRS qui lui reproche ses prises de position contre l'islamophobie[2] – auront ainsi contribué à un début de prise de

conscience au sein de la profession. Elle trouvera même une traduction éditoriale, à travers l'ouvrage collectif dirigé par le sociologue Sylvain Laurens et le philosophe Frédéric Neyrat intitulé *Enquêter, de quel droit ?* (2010). Constatant la multiplication des contraintes administratives justifiées au nom d'une éthique de la recherche souvent imposée de l'extérieur (par exemple par les organismes financeurs), ou de poursuites judiciaires menaçant, au-delà de l'enquête elle-même, la liberté d'expression des chercheurs, les auteurs y appelaient à la défense juridique des libertés académiques. Face aux multiples formes de surveillance susceptibles d'entraver les enquêtes en sciences sociales, ils proposaient notamment la création d'un droit à la protection des sources, modelé sur celle du secret des sources journalistiques.

3 Lors d'un colloque organisé à l'Institut d'études politiques d'Aix-en-Provence en mai 2018 et consacré aux formes de contrôle et de « mise en administration » des sciences sociales, les témoignages des participants se sont conjugués pour mettre en évidence le fait que, non seulement le constat dressé huit ans plus tôt dans l'ouvrage dirigé par Laurens et Neyrat était toujours d'actualité, mais que de nouvelles menaces s'étaient depuis matérialisées : recours toujours plus décomplexé à la contractualisation et aux enquêtes sur commande dans un contexte de précarisation croissante des métiers de la recherche[3] ; contraintes administratives liées à la protection des données personnelles et pressions à la publication de données sensibles dans le cadre des politiques d'*open data* ; permanence de la menace de procédures dites *bâillons*, lorsque des chercheurs sont poursuivis sur le terrain de la diffamation pour avoir contredit les représentations que les enquêtés voulaient donner d'eux-mêmes[4] ; menaces liées à l'extension du champ couvert par le secret, notamment au travers des législations récentes sur le secret des affaires[5].

4 S'agissant des processus de sécurisation associés à l'antiterrorisme, de jeunes doctorants ont également fait état, lors de ces journées, des difficultés à mener des enquêtes sur l'islam et les mouvements politiques associés. Certains sont ainsi dissuadés de travailler sur ces sujets, tandis que d'autres sont envoyés sur des terrains à risque sans préparation ni soutien suffisant et donc au péril de leur vie, avant d'être suspectés à leur retour par les services de renseignement. Sylvain Laurens est également revenu sur le cas édifiant de Thierry Dominici – qui fit l'objet d'écoutes judiciaires et d'une perquisition à son domicile en 2002 alors qu'il rédigeait une thèse sur le mouvement nationaliste corse –, passé inaperçu jusqu'à ce que le sociologue Marwan Mohammed en fasse état dans une tribune de 2015. Dans ce texte, ce dernier disait avoir lui-même renoncé à travailler sur la radicalisation par crainte d'attirer l'attention des autorités sur ses enquêtés[6].

5 Ces exemples illustrent les enquêtes ou les carrières entravées, les formes d'autocensure voire les traumatismes personnels que peut provoquer la surveillance d'État pour les chercheurs qui y sont exposés. La situation française est d'ailleurs loin d'être une exception, des évolutions semblables étant à l'œuvre aux États-Unis, au Royaume-Uni ou en Italie[7].

6 Deux tendances lourdes contribuent en effet à aggraver l'exposition des chercheurs en sciences sociales à cette surveillance : d'une part, la flambée antiterroriste et la criminalisation des mouvements sociaux qui, associés à l'évolution technologique, conduisent à démultiplier les capacités de surveillance des services de sécurité ; d'autre part, l'inanité des politiques numériques des établissements d'enseignement supérieur et de recherche, laquelle contribue à renforcer la dépendance des chercheurs vis-à-vis

d'oligopoles numériques toujours plus intégrés aux systèmes de surveillance étatique (Tréguer, 2019). Cet article dresse un état des lieux critique de la situation, avant de prodiguer quelques conseils quant aux contre-mesures permettant de réduire les risques que les données de la recherche ne soient exposées à la surveillance d'État.

La surveillance d'État à l'ère numérique

7 Les lois relatives au renseignement votées à la suite des attentats de janvier 2015 ont légalisé de nouvelles techniques de surveillance et élargi les finalités justifiant leur mise en œuvre par les services de renseignement, tandis que les lois antiterroristes – en particulier la loi du 3 juin 2016 – complétaient l'arsenal dont disposent les magistrats dans l'ordre judiciaire. Du côté des techniques de surveillance, la plupart peuvent donc désormais être mises en œuvre soit dans le cadre des pouvoirs de police administrative (en vertu du code de la sécurité intérieure), notamment par les services de renseignement, soit dans le cadre judiciaire (en vertu du code de procédure pénale), quoique pour des durées et des finalités qui diffèrent[8].

8 Un rapide survol de ces différents régimes de surveillance de données informatiques permet de saisir la diversité des mesures à disposition des autorités, lesquelles peuvent donc très bien concerner les données stockées ou traitées dans le cadre d'activités de recherche. Il y a d'abord ce qu'on désigne communément comme les *écoutes*, qui correspondent à la notion juridique d'interceptions de correspondances, déjà évoquées s'agissant du cas de Thierry Dominici. Elles peuvent s'exercer soit en temps réel, par exemple au travers de « bretelles » placées sur les réseaux des opérateurs afin de dédoubler le trafic Internet ou les appels téléphoniques de la cible[9], soit grâce à des réquisitions visant les correspondances stockées sur les serveurs d'un hébergeur (par exemple un fournisseur de messagerie électronique)[10]. La surveillance des données de connexion, ou métadonnées, renvoie à une catégorie plus large et très diverses d'informations traitées par les opérateurs : les autorités peuvent se contenter d'identifier l'abonné correspondant à un numéro de téléphone ou à une adresse IP, ou tâcher de déduire les activités et fréquentations d'une cible, par exemple à travers les facturations détaillées des communications[11] ou de ses relevés de géolocalisation[12].

9 À ces techniques classiques de surveillance des communications sont venues s'ajouter les perquisitions, ou saisies, de données numériques et de supports informatiques. D'abord légalisées dans le cadre judiciaire à partir de 2011[13], elles furent quasi systématiquement pratiquées lors des quelque 4 500 perquisitions administratives menées sous le sceau de l'état d'urgence décrété suite aux attentats de novembre 2015, et en vigueur pendant près de deux ans. En mai 2016, l'ancien directeur de la Direction générale de la sécurité intérieure (DGSI), indiquait ainsi aux députés de la Commission de la défense que « la moindre perquisition nous permet de récupérer des milliers de données ». Décrivant un service de renseignement débordé par la quantité de données à analyser, il précisait que « les entreprises françaises [...] ne sont pas encore capables de répondre à nos besoins, alors que nous devons acquérir ces Big Data immédiatement »[14]. Cela se traduira par un partenariat de près de deux ans entre la DGSI et l'entreprise américaine Palantir, spécialisée dans les applications sécuritaires de l'analyse massive de données. Faute d'informations fiables et en raison du secret d'État, il est difficile de mesurer le degré d'exposition des métiers de la recherche à ces perquisitions administratives. Le Défenseur des droits a toutefois révélé le cas d'un

chercheur l'ayant directement saisi après avoir été visé par une telle mesure. Dans un rapport au Parlement avare en détail, le Défenseur des droits indique seulement qu'il s'agissait d'un « chercheur militant contre la radicalisation islamiste, apparemment victime d'une erreur »[15]. Suite à la loi du 30 octobre 2017 transposant dans le droit commun diverses mesures associées à l'état d'urgence, les visites domiciliaires et les saisies administratives ont été intégrées au code de la sécurité intérieure[16]. Proche de ces mesures par sa nature extrêmement intrusive, la captation de données à distance au travers de techniques d'intrusion informatique est également possible, grâce aux diverses techniques de *hacking*. Pour les autorités, elles ont, à la différence des visites et saisies, le mérite de pouvoir être mises en œuvre à l'insu des personnes visées[17].

10 Enfin, pour compléter ce tableau des techniques dont dispose l'État pour surveiller communications et autres données numériques, il faut évoquer les dispositifs de surveillance massive et exploratoire dont s'est doté le renseignement français ces dix dernières années, et que la loi sur le renseignement 2015 est venue légaliser. En complément de la surveillance détaillée de quelques cibles identifiées évoquée ci-dessus, les agences de renseignement ont fait usage des dernières technologies informatiques pour mettre en œuvre des doctrines issues du monde militaire et fondées sur la détection de signaux faibles, c'est-à-dire de traces associées à des comportements suspects. Dans l'océan de données numériques qui circulent le long des réseaux, le but est de déceler, souvent en temps réel, des mots-clés, des identifiants, des signatures numériques et ce afin de mettre à jour, ainsi que l'affirmait un ministre français en 2015 à l'occasion du débat parlementaire, « des connexions à certaines heures, depuis certains lieux, sur certains sites [...] de repérer ainsi un trafic caractéristique »[18]. L'expérimentation de ces approches remonte au moins aux interceptions satellitaires dans les années 1980, sous l'égide de la Direction générale de la sécurité extérieure (DGSE). À partir de 2008, elles ont été étendues à Internet, au travers de puissants outils d'analyse du trafic placés dans les stations d'atterrissage des câbles sous-marins par lesquels transite le trafic Internet mondial. Le Premier ministre autorise ainsi la collecte de l'ensemble du trafic en provenance ou à destination d'une zone jugée sensible, typiquement le Maghreb, le Moyen-Orient, une grande partie de l'Afrique subsaharienne et des puissances comme la Russie, la Chine, l'Inde, ou les États-Unis[19]. De fait, les chercheurs travaillant sur les régions ou pays qui revêtent un intérêt stratégique pour le renseignement risquent de voir leurs communications glanées par ces outils de surveillance massive. Le renseignement intérieur a lui aussi commencé à s'approprier ces logiques de surveillance à grande échelle, au travers de machines installées sur les infrastructures des opérateurs télécoms et capables de scanner à la volée de larges portions du trafic Internet, dans le but d'identifier certains « sélecteurs » (des paramètres techniques censés repérer des communications suspectes)[20]. À l'inverse de la DGSE qui utilise les vastes moyens technologiques à sa disposition pour l'ensemble de ses missions, la DGSI n'est autorisée à les mobiliser que dans le cadre de la lutte antiterroriste. Ces outils peuvent par exemple être utilisés pour repérer des consultations de sites associés au terrorisme islamiste, ce qui là encore peut conduire les chercheurs qui se consacrent à ces questions à être considérés comme suspects et ciblés par les services.

11 Plus largement, la loi dresse la liste des « intérêts fondamentaux de la Nation » au nom desquels les diverses techniques de surveillance peuvent être employées, et fournit ainsi quelques indications sur les sujets de recherche les plus exposés à la surveillance. Le code de la sécurité intérieure évoque sept grandes finalités : l'indépendance

nationale, l'intégrité du territoire et la défense nationale (2 % des mesures de surveillance autorisées en 2018[21]) ; les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère (17 %) ; les intérêts économiques, industriels et scientifiques majeurs de la France (9 %) ; la prévention du terrorisme (45 %) ; la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, des violences collectives de nature à porter gravement atteinte à la paix publique (9 %) ; la prévention de la criminalité et de la délinquance organisées (17 %) ; la prévention de la prolifération des armes de destruction massive (1 %)[22].

12 Outre les zones et pays sensibles pour le renseignement, ces différentes thématiques donnent une idée des terrains à risque. Par exemple, une part significative de la finalité consacrée à la prévention des « violences collectives de nature à porter atteinte à la paix publique » est mobilisée pour justifier la surveillance de groupes dits *contestataires*. L'augmentation de son poids relatif entre 2017 et 2018 (de 6 % à 9 %) tient à l'importance de deux mouvements sociaux au cours de l'année 2018, à savoir la mobilisation autour de Notre-Dame des Landes en début d'année et le mouvement des « gilets jaunes » à partir du mois de novembre. La stratégie nationale du renseignement publiée par la présidence de la République à l'été 2019 fait d'ailleurs de la surveillance des « mouvements sociaux et [des] crises de société », ou encore « des affirmations de vie en société qui peuvent exacerber les tensions au sein du corps social », des priorités pour les années à venir[23]. Or, les données et communications collectées par les chercheurs enquêtant sur ce type de mouvements constituent évidemment des cibles de choix pour les services de renseignement. Le risque est d'autant plus grand que, sur le plan juridique, il n'est nul besoin qu'un soupçon plane sur une personne pour justifier une mesure de surveillance à son encontre : le fait qu'elle puisse fournir des informations utiles aux services suffit[24]. Au final, comme le résumait Marwan Mohammed en 2015 :

> Toute recherche qui touche la criminalité, qu'elle soit « ordinaire » ou organisée, les mouvements syndicaux, politiques et religieux, les différentes formes de radicalité militante, voire des domaines économiques, administratifs ou militaires considérés comme stratégiques, est susceptible d'entraîner une intrusion par les services. Ce qui fait beaucoup. Au-delà de cette loi [relative au renseignement], c'est la possibilité de produire des connaissances nouvelles en apportant des garanties aux personnes interrogées qui est en jeu. Les droits du chercheur et de « l'enquêté » sont liés dans les avancées scientifiques et donc les progrès théoriques en sciences humaines et sociales. (Mohammed, 2015)[25]

Dans l'ESR, des politiques numériques qui renforcent le risque de surveillance

13 Tandis que les capacités de surveillance des États se développent, multipliant ainsi les risques pour les chercheurs qui enquêtent sur des sujets ou des terrains « sensibles », les institutions de l'enseignement supérieur et de la recherche (ESR) semblent se désintéresser de ces enjeux. En dépit des discours lénifiants sur la souveraineté numérique repris aux plus hauts sommets de l'État, les politiques numériques dans l'ESR aboutissent souvent à une forme de démission. Sans même parler de la défense de droits nouveaux pour protéger les libertés académiques face à la surveillance d'État, on

trouve trop peu d'initiatives collectives ou de moyens dédiés à la formation des étudiants et des chercheurs pour protéger leurs données. Pire, nombre d'universités et de centres de recherche confient leurs infrastructures informatiques et leurs formations aux multinationales pionnières d'un « capitalisme de surveillance » fondé sur la collecte et l'exploitation de données personnelles à des fins de publicité ciblée[26]. Beaucoup d'établissements, y compris parmi les mieux dotés, ont ainsi cessé de développer, comme c'était souvent l'usage, des outils fondés sur des logiciels libres, conformes aux législations protectrices de la vie privée et administrés par des personnels de l'université conscients de leurs responsabilités en matière de protection des données (par exemple pour gérer des courriers électroniques et disposer d'espaces numériques de travail). En lieu et place, ils établissent des partenariats avec des acteurs comme Google ou Microsoft, accoutumant les étudiants, les chercheurs et l'ensemble des personnels aux produits et services de ces entreprises en position oligopolistique.

14 Outre le fait que ces pratiques n'apparaissent pas toujours conformes au droit à la protection des données personnelles[27], elles contribuent également à aggraver l'exposition des utilisateurs à la surveillance d'État – et pas seulement de la part des agences de renseignement des États-Unis, le pays où sont établies ces grandes entreprises. Ainsi, en mai 2015, lors d'une réunion conjointe à Paris, le gouvernement français annonçait la mise en place d'un point de contact avec les plateformes étasuniennes[28]. L'un des buts alors affichés consistait à ce que les réquisitions de données émanant des autorités françaises respectent bien au plan formel le droit américain auquel, hors procédure de coopération judiciaire internationale, ces multinationales restent soumises. Les acteurs privés s'engageaient alors à fournir des formations aux policiers et magistrats français. Ces échanges ont depuis permis d'accompagner la croissance rapide du nombre de données fournies par ces entreprises aux autorités françaises pour leurs activités de surveillance (entre 2013 et 2018, en croissance d'environ 430 % pour Google, 590 % pour Facebook – une augmentation encore plus rapide que celle observée aux États-Unis). À l'issue de cette réunion, ces entreprises ont également promis de tenir les autorités françaises informées des mises à jour qu'elles s'apprêteraient à déployer sur leurs services, en particulier celles qui risqueraient d'avoir une influence sur les capacités de surveillance de l'État – par exemple des dispositifs de chiffrement qui pourraient tenir en échec les programmes de cryptanalyse utilisés tant par les services de renseignement que par la police judiciaire.

15 La place croissante des grandes plateformes numériques dans l'ESR se traduit aussi par les formations qu'elles dispensent aux étudiants. À l'ère de la « start-up nation » – le projet vanté par certains responsables politiques pour propager les modèles de gestion et de management issus de la Silicon Valley à l'ensemble du champ bureaucratique (Algan et Cazenave, 2016[29]) – ces entreprises sont ainsi conviées dans les universités pour dispenser des cours en marketing digital aux étudiants. D'après Olivier Ertzscheid, maître de conférences en sciences de l'information, ces incursions témoignent du fait qu'« à tous les niveaux hiérarchiques et managériaux de nos universités, les plus inquiétants naufrages de nos missions de service public sont sacrifiées sur l'autel ripoliné de la "disruption" »[30]. Et bien qu'elles rencontrent des résistances[31], elles conduisent in fine à renforcer le poids de ces acteurs dans la gouvernance universitaire et, à terme, à valoriser des compétences les plus en phase avec les besoins en recrutement des secteurs économiques dont ils relèvent. Pour Ertzscheid, ces

rapprochements risquent ainsi d'aboutir à l'abandon des « valeurs et principes de l'université, en tout cas celles d'une université ouverte à tous et toutes, et surtout ouverte sur le monde (et pas uniquement sur le monde du patronat et de l'entreprise) ».

16 Tandis que les multinationales du numériques consolident leur alliance avec les pouvoirs publics, des associations comme Framasoft tentent de bâtir un contre-modèle. Leurs solutions alternatives aux Gafam, fondées sur un hébergement décentralisé et des logiciels libres, permettraient de répondre aux principaux usages quotidiens dans les métiers de l'ESR[32]. Pourtant, ces initiatives ne bénéficient d'aucun soutien institutionnel significatif. Framasoft, dotée d'un budget d'environ 350 000 euros, est financée à 94 % par les dons de quelque 4 000 donateurs. Avec ces ressources relativement modestes, l'association parvient à proposer ses services à près d'un demi-million d'utilisateurs chaque mois. Une démarche qui montre qu'avec un peu de volonté politique et de moyens, des services de qualité et répondant aux enjeux propres à l'ESR pourraient facilement devenir la norme.

Quelques bonnes pratiques à connaître pour protéger ses données

17 En dépit d'une prise de conscience croissante et d'initiatives isolées, l'enjeu de la protection des communications et des autres données associées aux activités de recherche en sciences sociales vis-à-vis de la surveillance d'État demeure à ce jour sans réponse satisfaisante au niveau institutionnel. Les appels à la reconnaissance de nouveaux droits en la matière restent lettre morte. À l'été 2015, lors de l'adoption de la loi relative au renseignement, le Conseil constitutionnel avait été saisi de ce texte préalablement à sa promulgation par des parlementaires et par le président de la République. Dans les mémoires transmis par certaines associations, il lui était demandé de reconnaître aux chercheurs le statut de profession protégée, au même titre que les journalistes ou avocats, auxquels certaines garanties spécifiques étaient accordées dans la loi[33]. Cela aurait également pu permettre de faire un premier pas vers la reconnaissance juridique d'un droit à la protection des sources pour les chercheurs. Mais le Conseil opposa alors une fin de non-recevoir, estimant que « le principe d'indépendance des enseignants-chercheurs n'implique pas [qu'ils doivent] bénéficier d'une protection particulière » face à la surveillance d'État[34].

18 En l'absence de protections juridiques spécifiques et en dépit du manque de soutien institutionnel, il est fondamental que nous puissions maîtriser des connaissances élémentaires en matière de sécurité informatique. Les bonnes pratiques et outils présentés ci-dessous, destinés à réduire les risques des différentes formes de surveillance dont peuvent faire l'objet les chercheurs en sciences sociales, ne constituent qu'un aperçu de ce champ complexe et sensible. Les lecteurs voulant en savoir davantage pourront utilement consulter des ouvrages de référence, comme le *Guide d'autodéfense numérique* (Collectif, 2017)[35], lire les quelques articles consacrés à la sécurité informatique dans le monde de la recherche (Aldridge *et al.*, 2010 ; Bendjaballah *et al.*, 2018), ou même consulter les trop rares acteurs associatifs qui dispensent des formations en la matière – et qui là encore ne bénéficient d'aucun soutien public –, à l'image de l'association Nothing2Hide[36].

Anticiper les risques

19 La première étape de toute approche en la matière consiste à savoir contre qui ou quoi l'on tente de se prémunir. Chaque cas relève d'enjeux spécifiques. Pour ce faire, il importe de construire ce qu'on appelle en sécurité informatique un « modèle de menace » et de répondre aux questions suivantes : Qu'est-ce que je cherche à protéger (s'agit-il de l'identité de mes sources, du contenu de mes notes de terrain, de la confidentialité de mes déplacements, etc.) ? Contre qui est-ce que je me protège (les services de renseignement, mes sources elles-mêmes, etc.) ? Quels sont les moyens (techniques, juridiques, etc.) que peuvent mobiliser ceux qui cherchent à accéder à mes données (enquête judiciaire, malveillance informatique, vol de mes appareils, etc.) ? Que se passera-t-il si j'échoue à protéger mes données (risque de garde à vue ; perte de l'anonymat de mes sources et poursuites judiciaires potentielles à leur encontre ; réprimandes de mon milieu professionnel, etc.) ? Et enfin, quelles sont les mesures (individuelles ou collectives) que je peux mobiliser pour minimiser ces risques (je peux me contenter d'anonymiser mes notes d'entretien, rechercher un conseil juridique ou prévenir mon entourage des risques encourus ; je peux souhaiter déployer des contre-mesures techniques – voir ci-dessous – ou même laisser mes appareils informatiques dans un lieu sûr lorsque je me rends dans un endroit « à risque » ; je peux décider de n'utiliser certains outils – tels que le courrier électronique fourni par l'université ou les réseaux sociaux – que pour certains usages et dans certaines circonstances, ou même privilégier le courrier postal plutôt que les communications numériques) ?

Sauvegardes, phrases de passe et chiffrement

20 Après l'anticipation des risques, il faut envisager les contre-mesures techniques, telles que le fait de chiffrer les disques durs de ses appareils, de procéder à des sauvegardes fréquentes ou d'adopter des « phrases de passe ». Sur les principaux systèmes d'exploitation, chiffrer le disque dur de son ordinateur ou de son *smartphone* est désormais non seulement possible mais aussi relativement aisé. Cela constitue une mesure de sécurité élémentaire, notamment au cas où un « adversaire » (une personne non autorisée qui chercherait à accéder à vos données) aurait physiquement accès à votre machine.

21 Ensuite, il est fondamental de procéder à des sauvegardes régulières de vos données sur des supports (disques durs, clés USB) qui soient eux-mêmes chiffrés. Selon leur degré de sensibilité, vos notes papier devront soit être placées en lieu sûr (par exemple dans un coffre) soit même détruites une fois informatisées et convenablement chiffrées. Sachez que la simple suppression de fichiers de votre disque dur ne suffit pas à les faire disparaître complètement (raison pour laquelle les services de l'État gérant des informations sensibles passent les disques durs dans des broyeurs d'autant plus fins que le niveau de classification des données qu'ils stockaient est élevé).

22 Enfin, pour chiffrer vos disques durs mais aussi pour vous authentifier sur de nombreux autres outils numériques, vous devrez le plus souvent choisir un mot de passe. Compte tenu du fait que la sécurité apportée par ce mot de passe – et notamment sa capacité à résister à des techniques de contournement ou de cryptanalyse – repose sur le nombre de caractères utilisés, il est fortement recommandé d'opter pour une « phrase de passe », qui soit suffisamment longue, aléatoire et peu connue pour ne pas

être devinée. Une méthode utile à cet égard est la méthode dite *diceware*, laquelle permet de générer aléatoirement une phrase de passe sûre et facile à mémoriser[37].

Outils utiles

23 Il est important d'utiliser des phrases de passe distinctes selon les usages, pour ne pas exposer l'ensemble de vos données et communications si l'une de ses phrases de passe venait à être compromise. Pour vous aider à gérer ces différents mots de passe, des applications comme Keepass[38] permettent de compiler de manière sécurisée vos différentes phrases de passe.

24 Afin d'apporter un niveau de sécurité supplémentaire à des dossiers ou fichiers sensibles stockés sur votre machine, vous pourrez utiliser Veracrypt[39], un logiciel qui permet d'y appliquer une couche supplémentaire de chiffrement tout en masquant leur présence sur votre disque dur. Pour anonymiser votre navigation Internet (notamment masquer votre adresse IP ainsi que la nature des sites visités), mais aussi pour contourner la censure de certains sites Internet, le logiciel de navigation TOR est également très utile, et ce en dépit des questions légitimes que pose la dépendance financière du projet TOR au gouvernement américain (Levine, 2018).

25 Pour chiffrer vos courriers électroniques, vous pourrez utiliser le protocole PGP, qui assure un chiffrement fort, dit *bout à bout*, entre vous et vos correspondants dès lors que ceux-ci l'utilisent également. En matière de messagerie instantanée (*chat*), le protocole IRC et le plug-in « off-the-record »[40], le protocole Matrix[41] ou l'application Signal assurent également un bon niveau de confidentialité, ces deux derniers disposant également de fonctionnalités « voix sur IP » permettant d'avoir des conversations téléphoniques.

26 Enfin, le système d'exploitation Tails vous permettra d'embarquer votre système d'exploitation sur une clé USB. Il suffit ensuite d'insérer cette clé sur n'importe quel ordinateur et de s'en servir comme disque de démarrage pour ne laisser aucune trace sur la machine en question. Tails offre également l'accès à différents logiciels (dont certains viennent d'être évoqués) reconnus pour leur capacité à préserver l'anonymat et la confidentialité des communications.

27 Attention cependant, même lorsqu'elle est bien utilisée, la cryptographie constitue une protection relative. Le chiffrement peut en effet être contourné de différentes manières (cryptanalyse, modèles d'attaque, ingénierie sociale, exploitation de failles de sécurité, etc.). Il existe aussi des failles juridiques : dans une décision d'avril 2018 allant à l'encontre du principe du droit à ne pas s'incriminer soi-même, le Conseil constitutionnel a estimé que, dans certaines conditions, une autorité judiciaire pouvait contraindre une personne à révéler ses « conventions de déchiffrement », une notion qui peut inclure les mots de passe. Cette disposition, l'article 434-15-2 du code pénal, punit le refus d'obtempérer de trois ans de prison et de 270 000 € d'amende[42]. Le ministère de l'Intérieur a tout de même relevé en 2018 près de 436 « refus de remettre aux autorités judiciaires ou de mettre en œuvre la convention secrète de déchiffrement d'un moyen de cryptologie », contre 82 en 2017 (des chiffres qui concernent notamment le refus de donner aux autorités le code de déverrouillage de son téléphone)[43].

28 En conclusion de cet état des lieux et de ces quelques conseils, soulignons également que, face au risque de surveillance, il faut savoir raison garder : les contre-mesures

envisagées doivent rester adaptées aux risques encourus. Il importe également de conjurer les formes d'autocensure qu'ils peuvent induire. Car le simple fait d'avoir conscience d'être potentiellement exposé à la surveillance peut suffire à produire des effets politiques délétères, par exemple en dissuadant les chercheurs de se pencher sur des sujets « à risque », ou en les conduisant à renoncer à certaines prises de parole. Il importe certes d'avoir conscience des risques et d'adapter ses comportements, sans pour autant sombrer dans une paranoïa qui serait paralysante. Surtout, il faut garder à l'esprit que toute solution de long terme aux problèmes que pose la surveillance d'État à la recherche en sciences sociales devra en passer par l'action collective. La prise de conscience de ces risques doit ainsi nous pousser à nous organiser, qu'il s'agisse de peser sur les choix de nos institutions respectives afin d'assurer une meilleure protection des données de la recherche, d'organiser des réseaux de soutien et de solidarité pour les chercheurs qui seraient directement victimes de telles mesures, ou encore de pousser nos associations professionnelles à se positionner sur ces enjeux dans le débat public.

BIBLIOGRAPHIE

ALDRIDGE Judith, MEDINA Juanjo et RALPHS Robert, 2010, « The problem of proliferation : guidelines for improving the security of qualitative data in a digital age », *Research Ethics*, vol. 6, n° 1, p. 3-9.

ALGAN Yann et CAZENAVE Thomas, 2016, *L'État en mode start-up*, Paris, Eyrolles.

BENDJABALLAH Selma, CARDOREL Sarah et FROMONT Émilie, 2018, « Anonymat et confidentialité des données qualitatives. Le retour d'expérience de beQuali », *La diffusion numérique des données en SHS. Guide de bonnes pratiques éthiques et juridiques*, V. Ginouvès et I. Gras éd., Presses universitaires de Provence.

CHIROLI Roberta, 2018, « Ora e sempre No Tav » [en ligne], *A.R.C.E. Bistrot des Ethnologues*, [URL : https://www.ethnobistro.fr/2018/03/roberta-chiroli-ora-e-sempre-no-tav/], consulté le 14 juin 2019.

COLLECTIF, 2017, *Guide d'autodéfense numérique*, Lyon, Tahin Party.

GLASER April, 2014, « 17 student groups pen open letters on the toxicity of mass surveillance to academic freedom » [en ligne], *Electronic Frontier Foundation*, [URL : https://www.eff.org/fr/deeplinks/2014/06/students-against-surveillance-17-university-groups-pen-open-letters-toxicity-mass], consulté le 12 juillet 2019.

KHAN Shamus, 2019, « The subpoena of ethnographic data », *Sociological Forum*, vol. 1, n° 34, p. 253-263.

LAURENS Sylvain et NEYRAT Frédéric éd., 2010, *Enquêter : de quel droit ? Menaces sur l'enquête en sciences sociales*, Bellecombe-en-Bauges, Éditions du Croquant.

LEVINE Yasha, 2018, *Surveillance Valley : The Secret Military History of the Internet*, New York, PublicAffairs.

O'DONNELL Aislinn, 2016, « Securitisation, counterterrorism and the silencing of dissent : the educational implications of prevent », *British Journal of Educational Studies*, vol. 64, n° 1, p. 53-76.

TANCZER Leonie Maria, MCCONVILLE Ryan et MAYNARD Peter, 2016, « Censorship and surveillance in the digital age : the technological challenges for academics », *Journal of Global Security Studies*, vol. 1, n° 4, p. 346-355.

TRÉGUER Félix, 2019, « Seeing like big tech : security assemblages, technology, and the future of state bureaucracy », *Data Politics : Worlds, Subjects, Rights*, D. Bigo, E. Isin et E. Ruppert éd., London, Routledge.

NOTES

1. Félix Tréguer est chercheur postdoctorant au CERI de Sciences Po, chercheur associé au Centre Internet et société du CNRS et membre fondateur de La Quadrature du Net, une association de défense des libertés publiques dans l'environnement numérique. Il est l'auteur de *L'utopie déchue. Une contre-histoire d'Internet (XV^e^-XXI^e^ siècles)* (Fayard, 2019).

2. Leclère Thierry, 9 juin 2009, « Vincent Geisser, un spécialiste de l'islam sous haute surveillance » [en ligne], *Télérama.fr*, [URL : https://www.telerama.fr/idees/vincent-geisser-un-specialiste-de-l-islam-sous-haute-surveillance,43918.php], consulté le 19 juin 2019. D'autres exemples sont fournis dans l'introduction de Laurens et Neyrat (2010).

3. Sur le recours croissant aux commandes dans la recherche en sciences sociales, voir les numéros 36 et 37 de la revue *Sociologies pratiques*, parus en 2018.

4. Michaut Cécile, 10 mars 2018, « Les chercheurs face aux "procédures bâillons" » [en ligne], Le Monde, [URL : https://www.lemonde.fr/idees/article/2018/03/10/les-chercheurs-face-aux-procedures-baillons_5268629_3232.html], consulté le 15 juillet 2019.

5. Le secret des affaires touche aux informations internes à une entreprise et dont les dirigeants cherchent à assurer la confidentialité. Voir la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, qui transpose en droit français la directive européenne 2016/943 du 8 juin 2016.

6. Mohammed Marwan, 2015, « Qui protège les chercheurs de la surveillance de l'État ? » [en ligne], *Libération.fr*, [URL : https://www.liberation.fr/debats/2015/11/08/qui-protege-les-chercheurs-de-la-surveillance-de-l-etat_1412098], consulté le 21 janvier 2019. Sur le cas Dominici, voir l'article de Marwan Mohammed dans ce numéro et Laurens Sylvain, 2016, « Des sciences sociales sous surveillance. Récit d'une enquête sociologique interrompue par un juge d'instruction » [en ligne], *Carnet de l'Association française de sociologie*, [URL : https://afs.hypotheses.org/108], consulté le 8 février 2019.

7. Voir, aux États-Unis, le témoignage de l'ethnographe américain Shamus Khan (2019) et d'April Glaser (2014). Sur le cas britannique, voir les critiques à l'encontre du programme antiterroriste Prevent et de ses ramifications dans l'enseignement supérieur et la recherche (O'Donnell, 2016). Sur le cas italien, voir l'exemple de Roberta Chiroli (2018), une anthropologue dont la thèse de doctorat portait sur l'opposition à la ligne à grande vitesse Lyon-Turin, et qui a été condamnée au pénal à deux mois de

prison avec sursis pour sa participation au mouvement de contestation, établie sur la base du recours au « nous participatif » dans sa thèse.

8. Pour approfondir, voir les rapports annuels de la Commission nationale de contrôle des techniques de renseignement et la circulaire du 2 décembre 2016 « de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée ».

9. Article L. 852-1 du code de la sécurité intérieure (renseignement) et l'article 100 du code de procédure pénale (judiciaire).

10. Notion du code de procédure pénale prévue à titre dérogatoire pour certaines catégories d'infractions (articles 706-95-1 et 706-95-2 du code de procédure pénale).

11. Il peut par exemple s'agir des fameuses fadettes, qui indiquent la liste des numéros appelés et appelants, la durée et la date des communications ou les relevés de connexions associées à un compte sur un service en ligne (par exemple, un réseau social comme Facebook ou Twitter). Article L. 851-1 du CSI (renseignement) et articles 60-1 et 60-2 (flagrance), 77-1-1, 77-1-2 (enquête préliminaire), 99-3 et 99-4 du code de procédure pénale (instruction).

12. L'accès aux données de géolocalisation peut se faire soit a posteriori, soit en temps réel. Dans le cadre du renseignement, cette dernière n'est autorisée que dans le cadre de la lutte antiterroriste (L. 851-2 du CSI). Dans le cadre judiciaire, la géolocalisation en temps réel est prévue aux articles 230-32 et suivants du code de procédure pénale.

13. Voir les article 57-1 (flagrance), 76-3 (préliminaire), 97-1 (instruction).

14. Audition de M. Patrick Calvar, directeur général de la sécurité intérieure (DGSI), 2016, Commission de la défense nationale et des forces armées, Paris, Assemblée Nationale, [URL : https://archive.fo/EznBo], consulté le 19 juin 2019.

15. Défenseurs des droits, 2016, *Bilan des saisines consécutives à l'état d'urgence et action du Défenseur des droits*, [URL : https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/note_conference_de_presse_etat_durgence.pdf], consulté le 19 juin 2019.

16. Article L. 229-5 du CSI (code de la sécurité intérieure).

17. Article L. 853-2 du CSI et articles 706-102-1 (préliminaire, flagrance) ou 706-102-2 (instruction) du code de procédure pénal.

18. Propos de Jean-Yves Le Drian, alors ministre de la Défense. Assemblée nationale, deuxième séance du mercredi 15 avril 2015.

19. Jauvert Vincent, 1er juillet 2015, « Comment la France écoute (aussi) le monde », *L'Obs*, [URL : http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html], consulté le 19 juin 2019.

20. Il s'agit des fameuses boîtes noires qui ont tant fait débat en 2015 (article L. 851-3 du CSI).

21. Commission nationale de contrôle des techniques de renseignement, 2019, *3e rapport d'activité 2018*, Paris, [URL : https://www.cnctr.fr/_downloads/NP_CNCTR_2019_rapport_annuel_2018.pdf], consulté le 19 juin 2019.

22. Article L. 811-3 du CSI.

23. Coordination nationale du renseignement et de la lutte contre le terrorisme, juillet 2019, *La stratégie nationale du renseignement*, présidence de la République, [URL :

http://www.sgdsn.gouv.fr/uploads/2019/07/20190703-cnrlt-np-strategie-nationale-renseignement.pdf], consulté le 6 août 2019.

24. L'article L. 811-3 se contente de prévoir que « les services spécialisés de renseignement peuvent recourir aux techniques [de renseignement] pour le recueil des renseignements relatifs » à l'un des intérêts légitimes. La loi autorise donc des mesures de surveillance pour toute personne qui serait susceptible de révéler des informations utiles à la poursuite de n'importe quelle finalité prévue à son article L. 811-3. Seul l'accès en temps réel aux données de connexion, prévu à l'article L. 852-1, requiert que toute personne concernée par ces mesures soit « susceptible d'être en lien avec une menace » terroriste, ou qu'elle fasse partie de l'entourage de personnes en lien avec une menace.

25. Mohammed Marwan, 2015, « Qui protège les chercheurs de la surveillance de l'État ? » [en ligne], *Libération.fr*, [URL : https://www.liberation.fr/debats/2015/11/08/qui-protege-les-chercheurs-de-la-surveillance-de-l-etat_1412098], consulté le 21 janvier 2019.

26. Shoshana Zuboff, 2019, « Un capitalisme de surveillance » [en ligne], *Le Monde diplomatique*, [URL : https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443], consulté le 27 avril 2020.

27. Les services de Sciences Po Paris, dont les outils numériques sont fondés sur la suite Google Apps, admettent ainsi que la conformité du stockage de fichier dans le Google Drive fourni aux étudiants et personnels de l'établissement est en conflit avec le règlement général européen relatif à la protection des données (RGPD), notamment parce que le stockage des données en Europe n'est nullement garanti par Google. Voir la page : « Hébergez [sic] ses données pendant ses recherches », *Sciences Po*, [URL : https://sciencespo.libguides.com/donnees-de-la-recherche/heberger-pendant], consulté le 3 septembre 2019.

28. Cassini Sandrine, 2015, « Terrorisme : accord entre la France et les géants du Net », *Les Échos*, [URL : http://www.lesechos.fr/journal20150423/lec2_high_tech_et_medias/02124922454-terrorisme-accord-entre-la-france-et-les-geants-du-net-1113723.php], consulté le 19 juin 2019.

29. Voir aussi Ertzscheid Olivier, juin 2017, « De la France comme une start-up nation », *affordance.info*, [URL : https://www.affordance.info/mon_weblog/2017/06/de-la-france-comme-une-start-up-nation-.html], consulté le 17 juillet 2017.

30. Ertzscheid Olivier, 2018, « Facebook forme les chômeurs, Google forme les étudiants. Et les universités vous emmerdent », *affordance.info*, [URL : https://www.affordance.info/mon_weblog/2018/02/facebook-google-universite-formation-et-merde.html], consulté le 17 juillet 2019.

31. Voir par exemple « Solidarité avec les profs de Paris 13 remplacés par Google », 28 février 2019, *La Quadrature du Net*, [URL : https://www.laquadrature.net/2019/02/28/solidarite-avec-les-profs-de-paris-13-remplaces-par-google/], consulté le 17 juillet 2019.

32. Nous indiquons ici quelques exemples des services proposés par les plateformes et pour lesquels Framasoft met en libre-service ses solutions alternatives : Google Doc : [URL : https://framapad.org/] ; Google Drive : [URL : https://framadrive.org/] ; Doodle : [URL : https://framadate.org] ; Dropbox : [URL : https://framadrop.org/] ; Slack ou Facebook Groups : [URL : https://framateam.org/] ; Google Form : [URL : https://

framaforms.org/] ; Skype : [URL : https://framatalk.org] ; services blog : [URL : https://frama.wiki/]. Pour le reste, voir : [URL : https://framasoft.fr/#topPgCloud].

33. En vertu de l'article L. 821-5-2 du CSI, les parlementaires, magistrats, avocats ou journalistes ne peuvent ainsi pas faire l'objet d'une mesure de surveillance « à raison de l'exercice de [leur] mandat ou de leur profession ». Le gouvernement ne peut pas non plus en passer par une « procédure d'urgence » pour autoriser les mesures de surveillance à leur encontre, laquelle lui permettrait de se passer de l'avis préalable de la Commission nationale de contrôle des techniques de renseignement (une protection qui ne s'applique pas en cas de contre-espionnage ou de terrorisme). Voir Les Exégètes amateurs, juin 2015, « *Amicus curiæ* transmis au Conseil constitutionnel dans le cadre des saisines visant la "loi relative au renseignement" », p. 102-103, [URL : https://exegetes.eu.org/recours/amicusrenseignement/2015-06-25-Amicus-Curiae-Version-Greffe-CC.pdf], consulté le 20 juin 2019.

34. Décision n° 2015-713 DC du 23 juillet 2015.

35. Voir aussi la version électronique du guide d'autodéfense numérique [URL : https://guide.boum.org/] ainsi que les tutoriels en ligne proposés par l'Electronic Frontier Foundation [URL : https://ssd.eff.org/fr].

36. Voir [URL : http://nothing2hide.org/].

37. Voir [URL : https://fr.wikipedia.org/wiki/Diceware].

38. Voir [URL : https://keepass.info/].

39. Voir [URL : https://www.veracrypt.fr].

40. Voir [URL : https://fr.wikipedia.org/wiki/Off-the-Record_Messaging].

41. Voir [URL : https://fr.wikipedia.org/wiki/Matrix_(protocole)].

42. La Quadrature du Net, 2018, « Le Conseil constitutionnel restreint le droit au chiffrement », [URL : https://www.laquadrature.net/2018/04/04/le-conseil-constitutionnel-restreint-le-droit-au-chiffrement/], consulté le 12 juillet 2019.

43. Castaner Christophe, 2019, « L'état de la menace liée au numérique en 2019 », [URL : http://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019], consulté le 12 juillet 2019.

RÉSUMÉS

Depuis les révélations de 2013 du lanceur d'alerte Edward Snowden sur les pratiques de surveillance des agences de renseignement occidentales, l'exposition du champ de la recherche en sciences sociales à la surveillance d'État – celle mise en œuvre par les appareils judiciaires et policiers, et plus largement justifiée par des impératifs de sécurité publique – a fait l'objet d'une attention croissante au niveau international. Deux tendances lourdes contribuent en effet à aggraver cette exposition : d'une part, la flambée antiterroriste et la criminalisation des mouvements sociaux qui, associés à l'évolution technologique, conduisent à démultiplier les capacités de surveillance des services de sécurité ; d'autre part, l'inanité des politiques numériques des établissements d'enseignement supérieur et de recherche, laquelle contribue à

renforcer la dépendance des chercheurs vis-à-vis d'oligopoles numériques toujours plus intégrés aux systèmes de surveillance étatique. Cet article dresse un état des lieux critique de la situation, avant de prodiguer quelques conseils quant aux contre-mesures permettant de réduire les risques que les données de la recherche ne soient exposées à la surveillance d'État.

Since the 2013 disclosures of whistleblower Edward Snowden on the surveillance practices of Western intelligence agencies, the exposure of the field of social science to state surveillance – implemented by judiciary and police authorities, and more broadly justified by public safety imperatives – has received growing attention at the international level. Two major trends contribute to worsening such exposure: on the one hand, the anti-terrorist tide and the criminalization of social movements which, combined with technological change, lead to a multiplication of the surveillance capacities of security services; on the other hand, the inanity of the digital policies of higher education and research institutions, which contributes to reinforcing researchers' dependence on digital oligopolies that are increasingly integrated into the State surveillance apparatus. This article provides a critical overview of the situation before dispensing some guidance on countermeasures aimed at reducing the risk that research data will be exposed to state surveillance.

INDEX

Mots-clés : surveillance, sciences sociales, protection des données, renseignement, sécurité informatique
Keywords : surveillance, social sciences, data protection, intelligence, computer security

AUTEURS

FÉLIX TRÉGUER

Politiste, Sciences Po, CERI

CAMILLE NOÛS

laboratoire Cogitamus