HAL open science

En France, des services de renseignement sans vrais contre-pouvoirs

Félix Tréguer

To cite this version:

Félix Tréguer. En France, des services de renseignement sans vrais contre-pouvoirs. 2021. hal-03952618

HAL Id: hal-03952618

https://sciencespo.hal.science/hal-03952618v1

Submitted on 23 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NoDerivatives 4.0 International License

En France, des services de renseignement sans vrais contre-pouvoirs

Tréguer, F. (2021, juin 27). *En France, des services de renseignement sans vrais contre-pouvoirs*. *The Conversation*. http://theconversation.com/en-france-des-services-de-renseignement-sans-vrais-contre-pouvoirs-163040

Huit ans après les révélations du lanceur d'alerte Edward Snowden, l'Assemblée nationale vient d'adopter, dans une relative indifférence, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. Le texte est désormais en cours d'examen au Sénat.

Il s'agit de la première révision d'ampleur de la loi renseignement adoptée en 2015. À l'époque, le gouvernement de Manuel Valls avait défendu cette loi en expliquantque la France était « l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal, cohérent et complet pour les activités de renseignement ». Le rapporteur de la loi à l'Assemblée, Jean-Jacques Urvoas, soulignaità l'envie combien elle constituait « un progrès de l'État de droit ». L'affaire était entendue : les services secrets voyaient leurs missions et leurs méthodes consacrées dans la loi ; le renseignement sortait autant que possible de « l'exceptionnalité » qui le caractérisait pour rentrer dans le rang des politiques publiques « normales ».

Cette manière de présenter les choses avait le mérite de reconnaître les lacunes historiques de la France en matière de contrôle des services de renseignement. Elle tendait cependant à faire oublier un important corollaire : le fait que la loi légalisait *a posteriori* des mesures de surveillance employées depuis des années en toute illégalité, ce qui aurait du valoir aux responsables politiques et administratifs ayant autorisé ces programmes des poursuites pénales.

Le projet de loi débattu en ce moment même au Sénat est certes bien moins ambitieux que son prédécesseur de 2015. Il relève cependant d'une même logique, bien analysée par les sociologues Laurent Bonelli, Hervé Rayner et Bernard Voutat, laquelle consiste à recourir au droit pour légitimer l'action des services et préserver leur autonomie au sein du champ bureaucratique. Menoeuvre manœuvre

Cette nouvelle loi cherche ainsi à sécuriser juridiquement des capacités de surveillance toujours plus étendues – telles les « boîtes noires » scannant le trafic Internet pour détecter des URL « suspectes » (article 13), le partage de données entre services français (article 7), ou l'obligation pour les opérateurs et gestionnaires de serveurs de collaborer avec les autorités pour « pirater » les messageries chiffrées (article 10), etc. – tout en abritant les services de renseignement de tout réel contre-pouvoir.

Renforcer le contrôle du renseignement devrait pourtant constituer une priorité compte tenu de sa place croissante au sein de l'État. Depuis 2015, les services de renseignement ont vu leurs effectifs augmenter de 30 %, notamment pour développer leurs capacités technologiques. Dans ce contexte, le recours aux différentes techniques de surveillance connaît lui aussi une forte croissance et porte sur des domaines toujours plus sensibles pour les libertés publiques. Ainsi, l'activité consacrée à la surveillance des mouvements sociaux – érigée en priorité depuis 2019 à la suite du mouvement des Gilets Jaunes – a plus que doublé en trois ans, passant de 6 % du total des mesures de surveillance en 2017 à plus de 14 % en 2020.

En dépit de cette montée en puissance, la quasi-totalité des propositions visant à renforcer les dispositifs de contrôle sont restées lettre mortes, et ce qu'elles émanent de la Délégation parlementaire au renseignement (la DPR, composée de députés et de sénateurs), de la CNIL (censée contrôler les fichiers dits « régaliens »), ou encore de la Commission de contrôle des techniques de renseignement (la CNCTR, qui rend des avis sur les mesures de surveillance sollicitées par les services).

Des échanges de données hors de tout contrôle

Depuis plusieurs années, la CNCTR demande par exemple de pouvoir contrôler le partage de données entre services de renseignement français et services étrangers. En France, la question est d'autant plus pressante que les flux de données échangés entre la Direction générale de la sécurité extérieure (DGSE) et la National Security Agency (NSA) ont connu une augmentation rapide suite à la conclusion de des accords SPINS, signés fin 2015 entre la France et les États-Unis. Or, la loi de 2015 excluait explicitement tout contrôle de la CNCTR sur ces collaborations internationales nourries par des réseaux de professionnels du renseignement jouissant d'une forte autonomie, et que Didier Bigo a proposé d'appréhender à travers la notion de « guilde transnationale ».

Dans son rapport annuel publié en 2019, la CNCTR admettait que ce véritable « trou noir » dans le contrôle du renseignement présentait un risque majeur, puisqu'il pourrait permettre aux services français de recevoir de leurs homologues des données qu'ils n'auraient pas pu se procurer légalement au travers des procédures définies dans la loi française. Dans le langage feutré qui la caractérise, la commission estimait qu'« une réflexion [devait] être menée sur l'encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers ».

Pour appuyer sa demande, la CNCTR évoquait la jurisprudence de la Cour européenne des droits de l'Homme (CEDH), laquelle a encore rappelé dans son arrêt Big Brother Watch c. Royaume-Uni du 25 mai 2021 que ces échanges devaient être encadrés par le droit national et soumis au contrôle d'une autorité indépendante (§ 362). Or, à ce jour, la France est aujourd'hui le dernierÉtat-membrede l'Union européenne à ne disposer d'aucun cadre juridique pour encadrer ces échanges internationaux. Ni le gouvernement ni les députés n'ont apparemment trouvé opportun d'y remédier.

La jurisprudence ignorée

Un autre principe essentiel dégagé par la jurisprudence européenne est le droit à l'information des personnes ayant fait l'objet d'une mesure de surveillance, dès lors qu'une telle information n'est plus de nature à entraver l'enquête menée à leur encontre par les services. Dans un rapport publié en janvier 2018, la CNCTR passait en revue la jurisprudence afférente et mentionnait plusieurs exemples de législations étrangères – la loi allemande notamment – garantissant une procédure de notification des personnes surveillées et prévoyant un certain nombre d'exceptions étroitement limitées. La CNCTR était forcée de constater que, en l'état du droit français, « les personnes surveillées ne peuvent être informées des techniques de renseignement mises en œuvre à leur encontre ». Le projet de loi élude complètement cet enjeu.

Le gouvernement a également écarté une autre exigence, encore rappelée par le Conseil d'État dans son arrêt du 21 avril 2021 relatif à la conservation généralisée des données de connexion. Dans cette décision qui donnait largement gain de cause au gouvernement, le Conseil d'État se fondait sur un arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020 pour exiger que les avis rendus par la CNCTR sur les mesures de surveillance soient « conformes » (c'est-à-dire impératifs pour le gouvernement) et non plus simplement consultatifs. La CNIL l'a à son tour rappelé début mai dans son avis rendu sur le projet de loi. Nouvelle fin de non-recevoir du gouvernement.

Quant à la volonté conjointe de la DPR et de la CNCTR de garantir à cette dernière un droit de regard sur les fichiers du renseignement, elle se heurte à l'opposition farouche des services. Comme l'ont souligné les parlementaires de la DPR, il s'agit pourtant d'une étape cruciale du contrôle, seule capable de permettre à la CNCTR de « s'assurer qu'aucune donnée n'a été recueillie, transcrite ou extraite en méconnaissance du cadre légal, voire en l'absence d'une autorisation accordée par le Premier ministre ».

On sera par ailleurs bien en peine de trouver, dans le cadre juridique français, des dispositions encadrant d'autres activités typiques du renseignement et extrêmement sensibles du point de vue des libertés publiques. C'est le cas de la surveillance des lettres et des colis postaux, ou encore de l'infiltration de certains groupes par des agents du renseignement. Au Royaume-Uni, l'Investigatory Powers Act de 2016 couvre pourtant ces deux domaines. Le loi française ne fait également aucune mention de la surveillance dite « en source ouverte », notamment sur les réseaux sociaux comme Facebook ou Twitter – une activité sur laquelle peu de choses ont fuité dans la presse mais dont on sait qu'elle a pris une importance croissante ces dix dernières années.

L'impossible transparence ?

Enfin, le texte aujourd'hui débattu au Parlement ne s'accompagne d'aucun progrès en matière de transparence des activités de renseignement, alors que l'étendue du secret obère gravement de la capacité des journalistes, des ONG, des chercheurs mais aussi d'autres acteurs institutionnels comme les juges à jouer leur rôle de contre-pouvoirs.

En dehors des quelques informations ayant filtré grâce au petit cercle de journalistes spécialisés ayant accès à des sources au sein des services, et outre les rares allusions faites concernant ces enjeux par les responsables du renseignement lors d'auditions parlementaires ou par la CNCTR, aucune information officielle n'est fournie sur la nature des technologies utilisées par les services et leur imbrication dans les processus de production du renseignement, sur les marchés publics et l'identité des sous-traitants privés, ni même sur les interprétations juridiques ayant cours au sein des services.

Là encore, la comparaison avec les principales puissances européennes du renseignement révèle en miroir le retard français. Il suffit pour s'en convaincre de consulter le rapport publié en août 2016 par David Anderson en marge du débat parlementaire sur l'Investigatory Powers Act. Ce juriste en charge du contrôle indépendant des législations antiterroristes y faisait état des capacités technologiques en matière de collecte et d'exploitation « massive » de données (« *bulk powers* »). Il donnait aussi plusieurs exemples de cas d'usage dans lesquels ces technologies étaient employées et évaluait leur intérêt opérationnel à partir de documents internes et d'entretiens avec certains hauts responsables.

En France, un tel degré de transparence semble pour l'heure inimaginable. Même si la CNCTR a fait quelques progrès dans la précision des informations fournies dans ses rapports, elle se contente pour l'essentiel de décrire l'état du droit et son évolution, ou de diffuser des statistiques générales sur les types de mesures autorisées et leurs finalités. On est encore loin du niveau de détail venant nourrir le débat public et alimenter les travaux des parlementaires, des journalistes ou des ONG dans des pays comme le Royaume-Uni ou l'Allemagne.

Faute pour le Sénat d'amender le projet de loi sur ces différents points, cette réforme constituera une nouvelle occasion manquée dans la tentative de réconcilier le renseignement français avec les normes internationales et les bonnes pratiques observées à l'étranger.