

NOTE FSU v2 : Projet de Loi sur le Renseignement

L'examen du projet de loi sur le renseignement a débuté devant l'Assemblée nationale le lundi 13 avril 2015. Il ne s'agit pas *stricto sensu* d'un texte « de circonstance » dans le sillage des attentats de janvier 2015 dans la mesure où il est en construction depuis près d'un an.

Les éléments de langage du Gouvernement s'inspirent néanmoins fortement du contexte. C'est d'ailleurs une première difficulté dans la mesure où le Gouvernement axe sa communication sur la menace terroriste, alors que ce projet de loi va, dans son contenu et sa portée, bien au-delà de la prévention des actes de terrorisme. En outre, le contexte a favorisé un relatif consensus dans la classe politique, pour ne pas dire une paralysie de cette dernière. Seule une poignée de parlementaires ont, jusqu'ici, émis des réserves sur certaines dispositions qui, en d'autres temps, auraient alimenté bien des polémiques.

Par ailleurs, c'est du fait de ce contexte que le Gouvernement s'est cru autorisé à activer la procédure d'urgence à l'occasion du débat parlementaire ; nous devons le regretter eu égard aux enjeux.

Le texte ne sera donc examiné qu'une fois en première lecture, par chacune des deux chambres. L'Assemblée nationale a adopté le texte le 5 mai (438 votes pour, 86 votes contre, 42 abstentions). Ce vote dépasse les clivages politiques classiques.

Le texte sera examiné au Sénat au cours de la première quinzaine de juin. La commission des lois du Sénat a déjà engagé ses travaux. L'Assemblée nationale aura le dernier mot, après réunion d'une commission mixte paritaire, dans l'hypothèse où le texte évoluerait entre les deux chambres (juillet).

Le texte a pour objectif d'offrir un cadre légal aux activités de renseignement, en rupture avec l'approche fragmentée qui était jusqu'alors mise en œuvre, dans un contexte d'absence de cadre légal pour nombre de techniques de renseignements pourtant mises en œuvre. Au-delà de la volonté affichée de régulariser des pratiques dont plus personne ne doute qu'elles ont été utilisées en dehors de tout contexte légal, ce texte élargit la finalité du renseignement.

En France, les principaux services chargés des opérations de renseignement sont la DGSE, la DRM et la DCRI. Pour apprécier de manière optimale la portée de ce texte, il convient de bien distinguer les pratiques ici examinées, qui s'inscrivent dans une démarche préventive dite de police administrative, de celles inscrites dans une démarche répressive, initiées par la police judiciaire, elle-même encadrée par l'autorité judiciaire. La police judiciaire a déjà, sous mandat du Juge, recours à la plupart des outils d'information évoqués dans le cadre de cette actualité. Cette confusion, et l'absence de délimitation stricte entre ces deux niveaux, est un autre problème majeur.

Champ d'intervention

- **Le renseignement, une activité devant obéir à des finalités ; au nombre de sept dans le projet de loi (art. L. 811-2) :**

*l'indépendance nationale, l'intégrité du territoire et la défense nationale.

*les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère.

*les intérêts économiques et scientifiques majeurs de la France.

*la prévention du terrorisme.

*la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale, ou de la reconstitution ou d'actions tendant au maintien de groupement dissous en application de l'article L 212-1.

*la prévention de la criminalité et de la délinquance organisées.

*la prévention de la prolifération des armes de destruction massive.

– **Des finalités décrites comme « relatives à la défense et à la promotion des intérêts publics ».**

La description des finalités a été modifiée en commission des lois à l'Assemblée nationale : là où le projet évoquait la seule défense des intérêts publics, la commission des lois évoquait la défense et la promotion des intérêts publics. Nous passons d'un renseignement « défensif » à un renseignement « offensif ». Comme évoqué en introduction, ce texte n'est donc pas centré sur la prévention des actes de terrorisme ; sa portée est bien plus large. C'est donc un piège que de se concentrer sur ce seul volet.

« *La prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale (...)* » est l'une des dispositions qui pose le plus grand nombre de difficultés. **La commission des lois de l'Assemblée nationale a amélioré le texte dans la mesure où le projet initial évoquait la « paix publique » en lieu et place de la « sécurité nationale ».**

Le risque susceptible de peser sur le mouvement syndical, militant, et sur l'activité politique était plus qu'évident. Le questionnement n'a toutefois pas totalement disparu avec la notion floue d'« *atteinte à la forme républicaine des institutions* », et, surtout l'interprétation susceptible d'être opérée quant aux « *violences collectives de nature à porter atteinte la sécurité nationale* ».

C'est l'éventualité de violences qui permettra aux services de renseignement d'avoir recours à la surveillance préventive des organisateurs de tout événement de nature collective. Mais personne ne pourra jamais garantir qu'un événement est insusceptible de déboucher sur des violences collectives, sauf à complètement verrouiller un événement par définition public et toucher, par ricochet, à la liberté de manifestation.

« *La prévention de la criminalité et de la délinquance organisée* » est une autre disposition qui pose des difficultés dans la mesure où cette finalité se confond avec celle de la police judiciaire, sous contrôle de l'autorité judiciaire, comme évoqué dans le paragraphe introductif. Au-delà de la confusion des rôles et des missions, cette disposition étend considérablement le champ d'action des services de renseignement spécialisés (DGSI..) ou non (services d'autres Ministères autorisés à avoir recours à l'arsenal du renseignement comme suit).

– **Des techniques de renseignement ne pouvant être mises en œuvre que par un nombre précis de Ministères :**

La mise en œuvre des techniques de renseignement est soumise à autorisation préalable du Premier Ministre (Art. L821-1). La demande est formulée « *par le ministre de la défense, le ministre de l'intérieur, le ministre de la Justice, ou les ministres chargés de l'économie, du budget ou des douanes* » (art. L821-2).

L'ajout du « ministre de la justice » est intervenu à l'occasion des travaux de la commission des lois de l'Assemblée nationale. C'est un décret en Conseil d'Etat qui doit préciser les services qui, au sein de chaque ministère, sont autorisés à mettre en œuvre les techniques de renseignement, ainsi que les finalités poursuivies.

Le texte issu de la commission des lois ne visait pas précisément l'Administration Pénitentiaire (AP), même s'il ne faisait aucun doute que l'AP était prioritairement concernée. Le texte finalement adopté le 5 mai mentionne l'AP, via la nécessité d'un décret spécifique (un second décret donc). Mais cette dernière mention, en plus de ne rien ôter au fond de ce qui est contesté, apporte toujours plus de confusion, avec une certaine redondance : en évoquant un décret spécifique pour définir les modalités de recours aux techniques de surveillance (alors même que l'alinéa 1er du même article le suggère déjà dans un premier décret), puis en prévoyant que ce décret spécifique définira les informations échangées entre l'AP et les services de renseignement spécialisés, tant pour les questions d'ordre et de sécurité des établissements que pour la défense et la promotion des intérêts publics listés dans la future loi...

Autoriser l'Administration Pénitentiaire, ou d'autres services du Ministère de la Justice, à mettre en œuvre des techniques de renseignement pose des difficultés : l'AP agit sous mandat de l'autorité judiciaire dans le cadre de la prise en charge des publics. L'autorité judiciaire est constitutionnellement garante des libertés individuelles. Il y a donc brouillage des frontières entre Justice et Ministère de l'Intérieur. Un Ministère garant du respect des libertés individuelles peut se retrouver prescripteur, en dehors du contrôle judiciaire, de mesures particulièrement attentatoires auxdites libertés.

De plus, la mise en œuvre de techniques de renseignement par des agents de l'AP pose une sérieuse difficulté quant à la mission de ces derniers, chargés non seulement de la garde des personnes détenues, de la sécurité des établissements (prévention des évasions et des attaques extérieures), mais aussi de leur réinsertion, de la recherche d'une adhésion de la personne avec la co-construction d'un parcours de l'exécution de peine dans un objectif de prévention de la récidive. Le lien de confiance, déjà fragile, sera pour le moins mis à mal.

Les auteurs de cette disposition indiquent que les personnels pénitentiaires qui auront recours aux instruments de surveillance ne seront pas les personnels en contact direct avec les personnes détenues. Mais, par expérience, nous savons qu'il sera impossible pour ces dernières de faire une quelconque distinction. En tout état de cause, recours à des outils particuliers ou non, l'ensemble des personnels est déjà invité à investir le champ de la surveillance, en lien avec l'actualité de la radicalisation violente.

Quel avenir pour les relations, déjà difficiles, entre des personnels de surveillance et les personnes incarcérées, lorsque ces dernières vivront avec le doute que celui avec lequel elles viennent d'échanger, aura profité de leur absence pour « sonoriser » cellule et parler.

Quel risque, à terme, pour les personnels pénitentiaires d'insertion et de probation dont on ne voit pas bien en quoi ils seraient, à terme, épargnés ? Au-delà des établissements pénitentiaires, les Services Pénitentiaires d'Insertion et de Probation (SPIP) seront-ils, à terme, concernés ? La loi ne fixe aucune limite, se contenant de renvoyer à un décret.

Les défenseurs du texte indiquent que la personne incarcérée ne doit pas, sur le champ de la surveillance, être mieux traitée que ne le serait le citoyen libre. Au-delà du fait que cette question peut être discutée et abordée différemment du fait que les pouvoirs de l'administration pénitentiaire sur la vie des personnes incarcérées sont déjà exorbitants, rien ne justifie que l'administration pénitentiaire doive sortir de son champ d'intervention premier **en faisant à la place** des services de renseignement spécialisés.

Bien plus, les services pénitentiaires pourraient avoir recours à l'ensemble des outils de renseignement pour chacune des 7 finalités définies ci-dessus. A titre d'exemple, quel lien entre l'AP et les intérêts économiques de la France ?

A l'occasion des débats, nous avons eu l'occasion de lire des contributions d'organisations syndicales de personnels pénitentiaires qui dépassent l'entendement, en évoquant l'intérêt d'une « *surveillance de l'environnement* » des personnes condamnées et des établissements : en l'occurrence, des organisations et associations engagées dans la défense des droits fondamentaux des personnes sous main de justice. De telles prises de position, par des organisations professionnelles particulièrement influentes au sein du Ministère de la Justice, peuvent légitimement nous faire craindre le pire.

Alors que les débats étaient engagés devant l'Assemblée, le Gouvernement a déposé un amendement pour que le Ministère de la Justice soit retiré de la liste des services susceptibles d'avoir recours, par eux-mêmes, aux dispositions prévues dans ce texte. Un autre amendement indiquait que seuls les services de renseignement spécialisés, en lien avec l'Administration Pénitentiaire, pouvaient avoir recours aux techniques de renseignement. Les deux amendements ont été rejetés par les députés le 14 avril.

Mise en œuvre

– Le Premier Ministre seul décideur

La mise en œuvre des techniques de renseignement est soumise à autorisation préalable du Premier Ministre. La demande précise la ou les techniques mises en œuvre, la ou les finalités poursuivies, le ou les motifs des mesures, la durée de validité, la personne, lieu ou véhicule concerné. Le Premier Ministre rend sa décision, valable pour une durée de 4 mois (au-delà, un renouvellement de demande est nécessaire).

L'ensemble du dispositif est placé entre les mains de l'exécutif, hors du contrôle du juge judiciaire, pour des mesures pourtant attentatoires aux libertés individuelles qu'il est constitutionnellement chargé de protéger.

Ce rôle prédominant confié au pouvoir politique est l'un des principaux points d'achoppement.

– La CNCTR : Commission Nationale de Contrôle des Techniques de Renseignement :

Il s'agit d'une autorité administrative indépendante, composée de 13 membres (contre 9 membres

prévus dans le projet initial) : 6 parlementaires (contre 4 initialement prévus), 3 magistrats de la Cour de cassation (contre 2 initialement prévus), 3 conseillers d'état (contre 2 initialement prévus), 1 personnalité qualifiée.

La CNCTR rend un avis sur toute demande d'utilisation de technique de renseignement transmise au Premier Ministre. Le délai pour rendre cet avis est de 24 heures (par le président de la CNCTR ou un des magistrats la composant). Si l'avis est rendu par un seul membre de la CNCTR, il est par la suite communiqué aux autres membres de la commission. Si la personne devant rendre l'avis doute de la validité de la demande, elle peut solliciter réunion de la Commission, qui doit alors rendre l'avis dans les 3 jours. **L'absence d'avis rendu vaut avis positif.**

L'avis négatif de la CNCTR prend la forme d'une recommandation, et ne lie pas le Premier Ministre.

La CNCTR est une structure ne pouvant rendre que des avis, qui risque de se trouver très rapidement « débordée » de multiples saisines. La procédure de contrôle instituée est inversée : un seul membre de la commission suffit pour donner un avis favorable, l'unanimité de la commission étant nécessaire pour émettre un avis défavorable (une recommandation).

Eu égard aux enjeux, c'est pourtant l'inverse qui s'impose.

– **La situation d'urgence :**

Les débats en séances plénière devant l'Assemblée nationale ont permis de revenir sur une disposition issue de la commission des lois hautement contestable. Les députés ont écarté la mise en œuvre d'une technique de renseignement par un chef de service ou une personne déléguée par lui, sans autorisation préalable du Premier Ministre, et sans avis préalable de la CNCTR. Cette procédure extraordinaire était prévue dans deux hypothèses : un cas d' « *urgence liée à une menace imminente* », ou un « *risque très élevé de ne pouvoir effectuer l'opération ultérieurement* ».

Le texte qui est soumis au Sénat revient finalement à la notion initialement portée au projet « *d'urgence absolue* », laquelle n'en reste pas moins obscure. La décision de recours aux techniques de renseignement n'est plus prise par un chef de service ou une personne déléguée par lui, mais par le Premier Ministre ou une personne déléguée par lui. Il reste que la CNCTR n'est toujours pas saisie en amont ; elle l'est a posteriori, dans un délai de 24 heures. Le fond du problème demeure tant sur la notion d'urgence que sur l'absence de saisine préalable de la CNCTR, alors que l'actuelle commission chargée de contrôler les interceptions de sécurité, saisie en amont, peut rendre un avis en deux heures.

Cette procédure n'est pas applicable lorsqu'est visé un lieu privé à usage d'habitation, ni si le recueil de renseignement porte sur une profession particulière (magistrat, presse, parlementaire, avocat).

– **Les contestations :**

* Par le CNCTR : de sa propre initiative ou sur réclamation d'une personne y ayant un intérêt direct et personnel, elle procède au contrôle des techniques invoquées, en vue de vérifier qu'elles ont été mises en œuvre dans le respect de la loi. La CNCTR notifie au demandeur de la réclamation qu'il a été procédé aux vérifications, sans confirmer ni infirmer leur mise en œuvre.

* Par le Conseil d'Etat : sur saisine de toute personne y ayant un intérêt direct et personnel, après qu'elle ait saisi la CNCTR, qui joue dès lors un rôle de filtre administratif, ou sur saisine du CNCTR. Le texte issu de la commission des lois ne prévoyait que la saisine du Conseil d'Etat en formation de jugement spécialisée. Les débats en séance plénière ont finalement permis d'envisager une saisine du Conseil d'Etat en formations (assemblée ou section) du contentieux de droit commun. Le Conseil d'Etat a le pouvoir, s'il constate une illégalité, d'annuler l'autorisation et d'ordonner la destruction des renseignements collectés irrégulièrement. Il peut saisir le Procureur de la République s'il estime que l'illégalité constatée est susceptible de caractériser une infraction.

La saisine du CNCTR ou du Conseil d'Etat par la personne visée par la technique de renseignement est illusoire, le plaignant se trouvant par définition dans l'ignorance des techniques de renseignement qui le concernent. Il n'aurait que peu d'éléments concrets pour établir un dossier et, éventuellement, demander réparation pour un préjudice qu'il ne pourrait correctement évaluer.

Le secret défense est, de par l'absence de définition dans ses limites, un obstacle majeur qui ne permettra pas au justiciable d'obtenir une réponse précise après qu'il ait fait état de ses doutes

sur un possible recours aux techniques de renseignement à son encontre, comme il limitera l'action des magistrats saisis en cas d'illégalité.

Les députés ont laissé entendre qu'ils avaient entendu les critiques, en gonflant l'effectif de la CNCTR. Mais la difficulté ne réside pas dans le nombre de membres, mais dans leur nature (des parlementaires, là où seuls des magistrats doivent pouvoir se prononcer sur le respect des libertés individuelles), et surtout dans la réalité du contrôle confié à cette autorité administrative indépendante (un véritable contrôle a priori, la nécessité d'un avis conforme).

A noter un amendement sur les « lanceurs d'alerte » finalement adopté, au cours des discussions en séance plénière, par l'Assemblée nationale (possibilité pour un agent d'interpeller, sous couvert de l'anonymat, la CNCTR).

Les techniques de renseignement

Les techniques de renseignement peuvent se classer en deux groupes : celles qui concernent le contexte d'un échange (accès à la possibilité de recueillir des données), et celles qui concernent le contenu des échanges (le recueil des données -voix, vidéo, écrits, etc...).

a) Les opérations de renseignement visant le contexte d'un échange :

*L'accès administratif aux données de connexion : cas de la personne identifiée par les services de renseignement :

Elles ne concernent pas le contenu des correspondances, mais l'ensemble du contexte d'un échange : contrat d'abonnement, adresse IP, adresse postale, lieu date et numéro de téléphone.

Aspirateur à données, sous deux réserves : la finalité de prévention du terrorisme, et des personnes préalablement identifiées comme présentant une menace. Les informations recueillies sont relatives à des personnes identifiées, ce ne signifiant pas qu'il s'agit d'informations émises ou reçues par elles, mais plus généralement des informations qui sont en relation avec elles. Les services de renseignement ont alors un accès « *en temps réel sur les réseaux des opérateurs* » : il n'y a plus de transmission sur demande mais un accès direct.

* La « possible » menace terroriste : cas de la personne non identifiée.

Art. L 851-4 : cet article est à l'origine de réactions fortes des FAI, opérateurs, etc... L'idée de cet article est de trouver une solution pour anticiper la menace terroriste. Nous nous trouvons dans le cas où cette menace n'est pas encore identifiée, pas représentée par un individu. La recherche de la menace se traduit par le biais d'une sorte de boîte noire imposée à tous les acteurs des nouvelles technologies, boîte noire décrite comme « *un dispositif destiné à détecter la menace terroriste sur la base de traitements automatisés* ».

L'objectif est d'aspirer l'ensemble des données dès lors qu'elles se rapportent à un algorithme préalablement établi. L'algorithme ne peut procéder à l'identification des personnes : il s'agira, dans le cas où l'algorithme enregistre une menace terroriste, de procéder (sur autorisation du Premier Ministre) à une identification de l'auteur. La CNCTR pourra émettre un avis sur le dispositif.

Au final, c'est un filet à données numériques que souhaite pouvoir poser le gouvernement, sans identification préalable des personnes visées. Filet d'une durée de 4 mois, renouvelable dès lors que subsiste une menace terroriste.

* La localisation en temps réel des personnes et des objets :

Elle peut être mise en œuvre dès lors qu'elle touche à l'une des sept finalités (non liées au seul terrorisme) : mouchards, etc... Sur autorisation du Premier Ministre, selon la procédure décrite plus haut.

* Le dispositif technique de proximité : IMSI Catcher.

Il s'agit d'un dispositif ayant pour objet d'aspirer des données de connexion afin d'identifier un équipement terminal ou le numéro d'abonnement de son utilisateur, et de géolocaliser l'équipement. Sur autorisation spécialement motivée du Premier Ministre, pendant une durée de 6 mois.

La difficulté se situe dans le fait que ces dispositifs de recueil d'informations couvrent un large périmètre du domaine public, y captant l'intégralité des données y transitant.

b) Les opérations de renseignement visant le contenu des échanges :

On se trouve au niveau des écoutes. Actuellement, ces interceptions de sécurité ont déjà une assiette large : elles ne doivent pas directement répondre à l'une des sept finalités, mais peuvent être autorisées dès lors qu'elles sont « *susceptibles de révéler des renseignements* » relatifs à l'une des sept finalités. Elles consistent principalement dans la sonorisation des lieux et véhicules, pose de mouchards informatiques. Ces outils de renseignement particulièrement intrusifs ne peuvent être autorisés que « subsidiairement » (si aucune des autres techniques ne permet d'obtenir les renseignements) et sont conditionnés par un avis express de la CNCTR (silence ne vaut donc pas autorisation dans ce cas).

L'autorisation est donnée par le Premier Ministre, pour une durée de deux mois.

Outre la possibilité de pose de micros dans des domiciles privés, la potentielle difficulté se porte au niveau des finalités de l'utilisation de cette technique de renseignement : elle peut être mise en œuvre sur chacune des sept finalités autorisant les techniques de renseignement, et non pas uniquement sur certaines d'entre elles (terrorisme ou lutte contre la prolifération des armes nucléaires par exemple).

Les débats en séance plénière, devant l'Assemblée nationale, ont conduit à une réduction des délais de conservation avant destruction des données collectées.

La place du Judiciaire :

In fine se pose la question du moment et des critères déterminant le passage d'une police administrative d'exception à une enquête judiciaire de droit commun, laquelle comporte des garanties pour ceux qui en sont l'objet. Le risque se situe au niveau de la mise à l'écart du Juge Judiciaire d'investigations portant sur des crimes ou délits dont l'élucidation relève de sa mission.

Vade mecum :

1° Des finalités trop large, et mal définies, pour le renseignement.

2° Une « communauté » du renseignement étendue qui génère une confusion des pouvoirs et des missions.

3° La prédominance du pouvoir exécutif au détriment du pouvoir judiciaire, garant du respect des libertés individuelles.

4° Une potentielle surveillance de masse.