Révision du code de procédure pénale 2016 : le nouveau régime des interceptions électroniques

Par Claudine Guerrier, professeure de droit à l'Institut des Mines/Télécom/Télécom École de Management/Litem, Claudine.guerrier@telecom-em.eu

Introduction

« L'État qui prétend éradiquer toute insécurité, même potentielle, est pris dans une spirale de l'exception, de la suspicion et de l'oppression qui peut aller jusqu'à la disparition plus ou moins complète des libertés »[1] explique Mireille Delmas-Marty, professeure de droit, qui mène depuis longtemps une réflexion sur les aspects nationaux et internationaux des droits de l'homme, notamment dans le contexte d'un « *monde dangereux* », pour revenir à l'un de ses titres les plus connus. Mireille Delmas-Marty a fait connaître, en décembre 2015 et janvier 2016, certaines réserves sur le projet de réforme du code de procédure pénale de 2016[2]. Cette loi de 120 articles ne présente pas un caractère de sécurisation juridique. Dans son avis concernant le projet de loi, la Commission Nationale Consultative des Droits de l'homme dénonçait « *la poursuite d'une politique de « replâtrage » ponctuelle … préférée à la conduite d'une réflexion d'ensemble sur l'architecture de la procédure pénale et de la sécurité intérieure, pourtant très attendue* [3]». Le Syndicat de la Magistrature[4] met en cause une procédure qui *« s'inscrit dans l'enchevêtrement de quatre textes, de réforme de la constitution, de prorogation de l'état d'urgence, de modification de ce régime et de modification de la procédure pénale* ». L'un des aspects de cette loi n° 2016-731 du 3 juin 2016 est la relative facilitation des interceptions électroniques et l'objet de cet article est d'examiner, dans ces dispositions, l'évolution de l'équilibre entre deux piliers de la Déclaration des droits de l'homme et du citoyen et la Déclaration universelle des droits de l'homme : la sécurité[5] et la liberté[6]. Le secret des correspondances est reconnu par la Convention européenne de sauvegarde des droits de l'homme[7] et la Charte européenne des droits de l'homme[8], dans le cadre du respect de la vie privée[9]. En France, plusieurs lois importantes sont intervenues dans ce domaine. La loi du 10 juillet 1991 a légiféré, après la condamnation par la CEDH de la France en 1990[10], sur les interceptions judiciaires et les interceptions de sécurité, dites administratives, en introduisant également un organisme de contrôle consultatif, la Commission nationale de contrôle des interceptions de sécurité (CNCIS). La loi dite Perben 2 du 9 mars 2004 fait apparaître dans le domaine des interceptions le Parquet, qui était

[1]Mireille Delmas-Marty, « *Libertés et sûreté dans un monde dangereux* », Paris, Éditions du Seuil, 2010, p. 141

[2]France Culture en décembre 2015 et janvier 2016 ; émissions « Du grain à moudre »

[3]Avis du 4 juin 2016, n° 69

[4]Audition par la Commission des lois, publiée le 12 février 2016

[5]Article quinze de la Déclaration universelle des droits de l'homme

[6]Article deux de la Déclaration des droits de l'homme et du citoyen

[7]Article huit de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

[8]Article sept de la Charte européenne des droits de l'homme

[9]Arrêt Malone c. Royaume-Uni, 2 août 1984, arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008, sur les données génétiques

[10]Arrêt Kruslin et arrêt Huvig, CEDH, 24 avril 1990

jusqu'alors exclu du domaine des interceptions. Le Parquet peut demander, pour certains crimes et délits commis en bande organisée, l'autorisation de procéder à des interceptions au stade des enquêtes préliminaires, autorisation qui est délivrée par le juge des libertés et de la détention du tribunal de grande instance. Au vingtième siècle et encore au début du vingt-et-unième siècle, le souci de préserver, dans la loi, conformément aux prescriptions du Conseil de l'Europe, l'équilibre entre liberté, respect des données à caractère personnel et sécurité est patent.

Depuis lors, un fléchissement se constate au profit de la sécurité, à l'époque où le monde globalisé utilise de plus en plus fréquemment des techniques de contrôle. Le *Patriot Act* a été adopté aux USA après les attentats du 11 septembre 2001. D'autres lois limitatives du secret des correspondances sont adoptées dans de nombreux pays occidentaux. En France, les lois se succèdent désormais : en 2004, est rendue possible la captation des images et des sons dans la loi dite Perben 2[11] : c'est encore le juge d'instruction qui délivre les autorisations. En 2006, la loi antiterroriste confie à la CNCIS le soin de nommer une personnalité « *qualifiée* » de contrôle en cas de stockage de certaines données de connexion par des agents spécifiques. La loi du 14 mars 2011 fonde, et ce malgré des débats animés, la captation des données informatiques à distance, qui est autorisée par le juge d'instruction.

En 2015, la loi sur le renseignement[12] modifie le paysage des interceptions : non seulement le nombre des personnes habilitées à effectuer des demandes est largement augmenté, mais les motifs sont considérablement élargis. La surveillance de masse, par des techniques évoluées, devient, dans certains cas, conforme au droit et approuvée par le Conseil constitutionnel. L'équilibre entre la sécurité et les libertés penche délibérément du côté de la sécurité, en s'appuyant sur le sentiment d'insécurité d'un grand nombre de citoyens. Le panoptique de Bentham n'est pas éloigné. Les attentats qui ont eu lieu sur le territoire français en janvier et novembre 2015, très médiatisés par les relais d'opinion publique, permettent au gouvernement de faire avancer des projets qui étaient étudiés depuis deux ou trois ans. La loi sur le renseignement est facilement adoptée et un projet de réforme de la procédure pénale portée initialement par la ministre Christiane Taubira se retrouve considérablement complété[13] par de nombreux dispositifs pénaux visant la lutte contre le terrorisme et la délinquance et le crime organisé. Après sa démission, ce texte sera porté par le nouveau Garde des Sceaux, Jean-Jacques Urvoas.

De plus, dans son avis sur le projet de loi, le Conseil d'État suggère d'introduire le terme « terrorisme » dans le titre du projet de loi, qui devient « *Projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale* ».

Cette nouvelle loi antiterroriste[14] est donc très vaste, divisée en trois titres, et comporte de nombreux volets. Le Conseil d'État considère qu'une certaine volonté d'équilibre apparaît dans le projet qui lui est soumis : y figurent une relative facilitation de certaines interceptions, mais aussi plusieurs garanties. Ainsi, on peut se demander si le Conseil d'État renoue véritablement avec

[11]Loi n° 2004-204 du 9 mars 2004

[12]Loi n° 2015-912 du 24 juillet 2015

[13]Par exemple, le dispositif des caméras mobiles devait initialement trouver une place dans la loi « *Égalité et Citoyenneté* ».

[14]*« Projet de loi renforçant la lutte contre la criminalité organisée et son financement, l'efficacité et les garanties de la procédure pénale* »

l'objectif de conciliation entre les impératifs de libertés individuelles et collectives. Les impératifs de sécurité s'appliquent à la lutte contre le crime organisé et le terrorisme. Ces impératifs ne doivent pas empiéter sur le respect des libertés qui risquent d'être affectées. Le Conseil d'État s'appuie dans son avis sur l'article 66 de la Constitution de la Cinquième République, concernant l'autorité judiciaire, gardienne des libertés individuelles, l'article deux de la Déclaration des droits de l'homme et du citoyen de 1789[15], l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, les articles 2 et 4 de la Déclaration des droits de l'homme de 1789 pour la liberté d'aller et de venir. Il n'en reste pas moins que ces exigences semblent plus difficiles à concilier dans le texte de la loi.

S'il approuve le plan dans son ensemble, le Conseil d'État est quelque peu réservé à l'égard de l'étude d'impact : il a effectué deux demandes de saisines rectificatives, à l'initiative de rapporteurs, mais n'est pas pleinement satisfait du travail effectué dans ce contexte. Font défaut, notamment, des données permettant de mieux apprécier l'utilité de certaines mesures, des études de droit comparé, avec références à des illustrations étrangères ou européennes, un état de droit complet[16]. La réserve concerne également dans une certaine mesure l'exposé des motifs : le Conseil d'État appelle de ses vœux une analyse plus riche[17]. Enfin, le Conseil d'État, dans son avis, recommande d'insérer les dispositions afférentes aux « *caméras piétons* », plus tard dénommées *« caméras mobiles »,* dans le Titre III, avec un chapitre autonome, au lieu de les laisser insérées dans le Titre I, consacré aux communications électroniques. Cela sera suivi d'effet[18]. Si les interceptions sont facilitées (I), des garanties sont officiellement envisagées (II).

I – Un élargissement conséquent des possibilités de captations ou d'interceptions

C'est le cas de la sonorisation ou surveillance vidéo d'un lieu ou d'un domicile ou encore du recours à des dispositifs de surveillance des téléphones mobiles dits "IMSI CATCHER".

A) La sonorisation et la surveillance vidéo régies jusque-là par la loi Perben 2.

L'article du code de procédure pénale visé était l'article 706-96 ; il est complété par l'article 706-96-1 et concerne les motifs de la délinquance et de la criminalité organisée.

Ces captations sont possibles au stade de l'enquête en matière de criminalité organisée. Le nouvel article dispose que, sur requête du procureur de la République, le juge des libertés et de la détention peut les autoriser pour une durée d'un mois, renouvelable une fois.

Le juge d'instruction peut autoriser l'introduction dans un lieu ou un véhicule privé, y compris à l'insu du propriétaire ou sans le consentement du propriétaire ou du légitime occupant, d'un dispositif de

[15]Quatre droits naturels : liberté, propriété, sûreté, résistance à l'oppression

[16]Le Conseil d'État emploie même l'expression « *lacunaire* » pour qualifier l'état de droit

[17]Cela permettrait de *« mieux appréhender, en les replaçant dans une perspective historique, les nouveaux équilibres résultant du texte entre police administrative et police judiciaire, d'une part, et entre parquet, juge d'instruction et juge des libertés et de la détention, d'autre part* », Conseil d'État, avis du 28 janvier 2016

[18]*« … La disposition relative aux "caméras piétons" qui ne lui a pas paru, compte tenu des finalités de ce dispositif notamment en matière de preuve, trouver sa place dans le titre I consacré à la lutte contre le crime organisé et le terrorisme. Il a en conséquence inséré cet article dans le titre III, en lui affectant un chapitre autonome »*, Conseil d'État, avis du 28 janvier 2016

captation des images et des sons. S'il s'agit d'un lieu d'habitation, l'introduction de nuit d'un dispositif technique doit être autorisée par le juge des libertés et de la détention, saisi par le juge d'instruction. Les locaux d'entreprises de presse, d'avocats, de médecins, de notaires, d'huissiers, sont exclus de ce dispositif. La décision est prise pour une durée maximale de deux mois, et ne peut excéder deux ans.

B) Le recours aux « *caméras piétons* » ou « *caméras mobiles* »

1. Un nouveau dispositif en droit français

En France, les caméras piétons portées par des policiers sont expérimentées depuis 2013 dans certaines zones de sécurité prioritaires. Elles devraient permettre de réduire les violences exercées à l'encontre des agents publics et les contestations ultérieures par les personnes physiques. Elles ont été intégrées dans la réforme sur le code de procédure pénale, mais auraient pu trouver leur place dans d'autres lois.

La captation des images et des sons par les agents de police et de gendarmerie équipés de caméras individuelles est autorisée pour les agents équipés de ces matériels lorsqu'un incident se produit ou serait susceptible de se produire[19]. Elle peut intervenir dans tous les lieux publics ou privés où apparaissent aussi les personnels habilités, y compris dans le domicile privé des personnes lorsque cela est permis.

La finalité des dispositifs consiste autant à prévenir les incidents qui pourraient survenir pendant le déroulement de ces interventions, qu'à contribuer à la répression des infractions recherchées lors de ces interventions par la collecte de preuves qui seront utilisées dans le cadre de procédures pénales, administratives ou disciplinaires. L'enregistrement ne peut se faire en continu, contrairement à ce qui est prévu pour la vidéoprotection. L'usage des « *caméras piétons* » est bien distinct de la vidéoprotection[20] ; il constitue un outil relativement nouveau. La caméra portative, appelée « *caméra mobile* » dans la loi définitivement adoptée (chapitre deux) est fixée sur l'habit d'un policier ou d'un gendarme pour filmer les interventions dans les lieux publics. L'article 32 du Titre III clarifie le cadre légal à l'usage de caméras mobiles par les forces de l'ordre, pour empêcher les incidents susceptibles de se produire à l'occasion d'interventions policières ou militaires. Durant des discussions à l'Assemblée nationale, un amendement adopté permettait une utilisation des caméras dès qu'une personne concernée par une intervention des forces de l'ordre en fait la demande. Au Sénat, cette possibilité disparaît. Dans le texte définitif, il est indiqué qu'un décret en Conseil d'État interviendra pour préciser les modalités d'utilisation des données recueillies par les caméras mobiles. Dans la mesure où la captation de tels images et sons se produit dans des lieux publics ou privés, il est de nature à porter atteinte au respect de la vie privée. La loi offre cependant des garanties. Les caméras sont portées de façon apparente, comportent un signal visible qui fait connaître l'enregistrement et doivent donner lieu, sauf circonstances spécifiques, à une information des personnes enregistrées. Les personnels qui bénéficient des caméras mobiles ne peuvent avoir accès directement aux enregistrements auxquels ils procèdent. Les enregistrements, sauf s'ils sont utilisés dans le cadre d'une procédure judiciaire, administrative, disciplinaire[21], sont effacés au bout de six mois. À titre

[19]Article L. 241-1

[20]Titre V du livre II du code de la sécurité intérieure

[21]Les procédures disciplinaires s'inscrivent dans le cadre du droit disciplinaire, qui fixe des sanctions en cas de comportements fautifs commis par des personnes physiques dépendant de la même structure. Le droit disciplinaire est une

expérimental, pour une durée de deux ans à compter de la promulgation de la loi, le Gouvernement est en mesure d'autoriser les agents de police municipale à procéder, au moyen de caméras individuelles, à un enregistrement audiovisuel de leurs interventions.

2. Un dispositif à l'efficacité discutée

Entrées en vigueur aux USA, les caméras piétons donnent lieu à des débats quant à leurs résultats : vues par certains comme des instruments de pacification, elles seraient pour d'autres coûteuses et peu utiles.

Dans son avis préalable, le Conseil d'État s'est posé la question de la conformité de cet outil aux impératifs de liberté et s'est demandé si le procédé est en mesure de porter atteinte au respect de la vie privée. Il mentionne l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789[22], l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, l'arrêt de la CEDH S. et Marper c. Royaume-Uni du 26 mars 1987[23], les articles 7 et 8 de la Charte européenne des droits fondamentaux de l'Union européenne. Malgré la prise en compte de la jurisprudence et de ces textes, le Conseil d'État estime que le recours aux caméras piétons est justifié par un motif d'intérêt général[24] et que la mise en œuvre est proportionnée aux objectifs. Des garanties sont indispensables : les personnes filmées sont informées de la captation de leur image ; les agents équipés de caméras sont dans l'impossibilité d'accéder eux-mêmes aux images. Dans ces conditions, le Conseil d'État considère que l'usage des caméras piétons est conforme à la jurisprudence du Conseil constitutionnel. Il s'agit d'une ingérence prévue par la loi, avec un caractère de nécessité dans une société démocratique qui obéit aux exigences de la jurisprudence de la CEDH. Devant le Sénat, se pose la question de durée de conservation, qui est de six mois, au lieu d'un seul pour la vidéoprotection. Cette différence ne semble pas anormale au ministre Bernard Cazeneuve[25], mais les parlementaires ne sont pas convaincus et ramènent le délai de conservation de six mois à un mois. Le texte définitif revient finalement à six mois.

C) L'usage d'IMSI Catcher

L'utilisation d'IMSI Catcher pour les interceptions administratives a été introduite dans la loi sur le renseignement[26]. Les IMSI Catcher, fausses antennes relais, peuvent en particulier capter les données de connexion transmises entre le périphérique électronique, notamment un téléphone portable, et la

---

branche du droit administratif, mais entretient aussi des relations avec le droit pénal. Le droit disciplinaire garantit les droits de la défense

[22]Décision n° 94-352 DC du 18 janvier 1995 : décision du Conseil constitutionnel afférente à la loi d'orientation et de programmation relative à la sécurité dans ses articles 10, 16, 18. L'article 10 établit un régime d'autorisation et d'utilisation des installations de systèmes de vidéosurveillance. L'article 16 insère un article 2 bis dans le décret du 23 octobre 1995 ; des fouilles de véhicules sont autorisées. Le Conseil constitutionnel estime que sont contraires à la Constitution, dans l'article 10 «*L'autorisation sollicitée est réputée acquise à défaut de réponse dans un délai de 4 mois* », à l'article 16, le deuxième alinéa « être utilisés comme projectile », ainsi que les troisième et quatrième alinéas.

[23]Sur l'effacement des données à caractère personnel : la conservation illimitée des données de personnes non condamnées est reconnue comme une violation de la vie privée

[24]Prévention des atteintes à l'ordre public et leur éventuelle répression

[25]Bernard Cazeneuve, Sénat, séance du 29 mars 2016 : *« Si cette durée est plus longue que pour les images de vidéoprotection, elle n'est pas disproportionnée à l'objectif poursuivi* »

[26]Loi n° 2015-912 du 24 juillet 2015

véritable antenne relais. Dans certaines conditions, ce procédé permet également d'accéder au contenu des correspondances. En matière de renseignement, l'autorisation est délivrée par la seule personne habilitée pour ces interceptions, le Premier ministre, après avis simple de la Commission nationale de contrôle des techniques de renseignement (CNCTR) pour une durée de quatre mois. Dans le domaine judiciaire, l'usage des IMSI Catcher peut intervenir sur la base des nouveaux articles 706-95-4 à 706-95-10 du code de procédure pénale, qui s'applique à toutes les infractions correspondant à la criminalité organisée et pas les seules infractions terroristes.

Dans le domaine administratif, c'est au juge des libertés et de la détention, dans le cadre d'une enquête, d'autoriser, sur requête du Procureur de la République, cette interception. Le juge autorise l'utilisation d'un dispositif technique qui permet d'identifier le terminal, le numéro d'abonnement. L'autorisation est délivrée pour un mois, et est renouvelable une fois. En cas d'urgence, c'est le procureur de la République qui donne cette autorisation, qui est confirmée par le juge des libertés et de la détention dans les vingt-quatre heures.

Dans le cadre d'une instruction, la durée de l'autorisation délivrée par le juge d'instruction est de deux mois, renouvelable trois fois. Lorsqu'il s'agit d'interceptions des correspondances émises ou reçues par un équipement terminal, la durée de l'autorisation donnée par le juge des libertés ou de la détention ou le juge d'instruction est de quarante-huit heures, renouvelable une fois.

L'ordonnance est motivée et n'est pas susceptible de recours.

D) La captation des données informatiques

En matière judiciaire elle est élargie aux données stockées sur un ordinateur et non plus simplement aux données telles qu'elles s'affichent sur l'écran, comme cela est déjà permis pour les services de renseignement.

En matière administrative, les dispositifs techniques sont soumis à un régime d'autorisation administrative dépendant de l'Agence nationale de sécurité des systèmes d'information (ANSSI). Dans le cadre de l'enquête, l'autorisation délivrée par le juge des libertés et de la détention vaut pour un mois, renouvelable une fois. Dans le cadre de l'instruction, la décision du juge d'instruction vaut pour quatre mois, renouvelable sans que la durée totale ne puisse dépasser deux ans.

II – Quelques garanties néanmoins limitées

A) Le rôle du procureur de la République comme directeur d'enquête est clairement identifié.

Cela a amené de vives discussions entre les divers acteurs du débat, parlementaires, autorités administratives indépendantes, opérateurs. Le Syndicat de la Magistrature s'est interrogé sur la qualité d'un texte dans lequel le parquet dispose de davantage de prérogatives, alors que c'est l'institution judiciaire qui garantit une procédure contradictoire avec un juge indépendant. L'article 54 de la loi du 3 juin 2016 crée un nouvel article 39-3 dans le code de procédure pénale, afférant aux attributions du procureur de la République. Ce dernier adresse des instructions à caractère général ou particulier aux enquêteurs. Il contrôle la légalité des moyens utilisés par les enquêteurs, la proportionnalité des dispositifs d'investigation en fonction de la gravité des faits. L'alinéa 2 indique

que les investigations tendent à la manifestation de la vérité et respectent les droits de la victime et de la défense. Le procureur n'est pas une autorité judiciaire au sens de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il semble s'apparenter à un juge et l'évolution du rôle du procureur, notamment en matière de criminalité organisée, sera peut-être bientôt à nouveau à l'ordre du jour. Il n'est cependant pas certain que l'évolution de ce rôle contribue aux libertés publiques.

B) La durée

Les procédures d'interceptions téléphoniques qui sont décidées au cours de l'instruction devront faire l'objet d'une motivation[27] et sont limitées par catégories selon certains délais. Le Conseil d'État souhaitait faire compléter ces dispositions et a été suivi par le législateur :

- Une différenciation des durées pendant lesquelles le juge d'instruction et le procureur de la République sont respectivement susceptibles de recourir à la sonorisation ou à la fixation d'images et à la captation de données informatiques : le juge d'instruction peut imposer ces techniques pour une durée de quatre mois[28] alors que le procureur de la République ne peut y recourir que pour une durée d'un mois. Ces durées sont pleinement conciliables avec celles qui ont été prévues pour les interceptions de télécommunications et pour la géolocalisation[29].

- Une limite maximale à la durée du recours à la sonorisation ou la fixation d'images et à la captation des données informatiques est fixée à deux mois en enquête préliminaire et à deux ans pour l'instruction. La durée maximale de deux mois en enquête préliminaire correspond avec la durée introduite par la loi LOPPSI 2 pour les interceptions de télécommunications en matière de délinquance et de criminalité organisées. Le Conseil d'État considère, y compris pour la captation des données informatiques à distance qu'une telle durée était proportionnée à la gravité des infractions envisagées.

L'harmonisation des durées peut être souhaitée, mais ce souhait n'est pas réaliste, car les durées dans le domaine des interceptions et des captations ont toujours varié, et, dans le contexte actuel, les décrets en Conseil d'État sont tout prêts à épouser variations et évolutions techniques et juridiques.

C) Les « personnalités protégées » en matière d'écoutes

Les écoutes concernant les députés et les sénateurs, les magistrats et les avocats ne sont possibles que s'il existe des motifs sérieux, « *plausibles* » de soupçonner que l'une de ces personnalités a participé, soit à titre d'auteur, soit en tant que complice, à la commission de l'infraction. Les écoutes ne pourront être décidées que par décision motivée du juge des libertés et de la détention saisi par ordonnance motivée du juge d'instruction. L'ordonnance du juge d'instruction et la décision du juge des libertés et de la détention constituent une double garantie, ce qui n'existait pas auparavant. Le Conseil d'État apporte son approbation à ce double examen qui a été auparavant admis à deux reprises pour la géolocalisation[30] et dans le cadre du projet de loi renforçant la protection du secret

[27]Ce qui n'était pas obligatoire antérieurement

[28]Durée traditionnelle en matière d'interceptions

[29]Articles 100-2 et 706-95 du code de procédure pénale.

[30]Article 230-34 du code de procédure pénale

des sources des journalistes[31]. Le Conseil d'État considère que ces dispositions renforcent le principe de la séparation des pouvoirs[32], de l'indépendance des magistrats et du secret des délibérés et les droits de la défense. De plus, d'éventuelles nullités afférentes à la procédure peuvent être sanctionnées par la chambre de l'instruction.

D) La plateforme nationale des interceptions judiciaires

Depuis le début de sa mise en place, la Plateforme nationale des interceptions judiciaires (PNIJ) attire des critiques. La loi consacre cette plateforme, lui dédiant le Chapitre VI du nouveau code de procédure pénale, qui doit entrer en vigueur le 1er janvier 2017[33] et ce malgré un réel besoin d'amélioration du système des interceptions. En effet, la PNIJ a connu des dysfonctionnements : elle a fait l'objet d'un travail de conception en 2005 ; le marché passé pour sa conception et sa réalisation commence en 2011, il ne devrait se terminer, selon la PNIJ elle-même, qu'à la fin 2016. La Cour des comptes regrette que la plateforme soit hébergée, non pas par l'État, mais par une société commerciale, Thales[34] : « *L'État a préféré faire le choix d'un degré élevé de dépendance* » en *« ignorant les possibilités de coopérations interministérielles pour l'hébergement et pour l'exploitation de ce système* ». La Cour des comptes met l'accent sur les bienfaits d'une mutualisation des services d'interceptions administratives et judiciaires. L'article 230-45 du code de procédure pénale prévoit aussi que cette PNIJ a pour mission principale de centraliser l'exécution des réquisitions et demandes d'interceptions. Un décret en Conseil d'État, pris après avis public et motivé de la CNIL, pour protéger les libertés individuelles, est le nœud gordien de l'article 88 de la loi. Mais la loi elle-même ne développe pas le rôle de la PNIJ, sans doute en raison des incertitudes politiques et financières qui ont jalonné la très progressive mise en place de cette plateforme.

E) Les garanties concernant les IMSI Catcher

Devant les critiques afférentes aux IMSI Catcher, des tentatives d'encadrement voient le jour, mais sont rejetées

1. Le rejet de l'encadrement

Cette nouvelle méthode d'interception est indiscriminée ; elle permet de collecter des informations multiples et sur des personnes étrangères à l'affaire en cause. De nombreux amendements visant à encadrer ces dispositifs et à limiter d'éventuelles dérives avaient été déposés durant les discussions parlementaires. Ils n'ont toutefois pas été adoptés, car considérés par le gouvernement comme inadaptés aux objectifs de la loi.

Ainsi, devant l'Assemblée nationale est repoussé un amendement[35] tendant à encadrer fortement les finalités de l'IMSI catcher qui devraient se limiter à la recherche et à la constatation des infractions

[31]Loi actuelle 2010-1 du 4 janvier 2010

[32]Article 16 de la Déclaration des droits de l'homme et du citoyen

[33]Article 88 de la loi du 13 juin 2016

[34]Cour des comptes, 21 avril 2016 : *« En particulier, nous n'avons pu déterminer avec certitude les raisons qui ont conduit le ministère de l'Intérieur à refuser d'installer la Plateforme dans l'un de ses sites informatiques sécurisés, alors même que des études conduites préalablement avaient formulé des recommandations en ce sens »*

[35]N° 361, Assemblée nationale, première séance du 3 mars 2016

pour lesquelles son usage a été permis par le juge des libertés et de la détention ou par le juge d'instruction[36] et en exclure des infractions qui pourraient être découvertes par ce biais. Est également repoussé un amendement[37]apportant des garanties au recueil des données décidé en urgence sur autorisation du procureur de la République. Les données auraient été centralisées, conservées, détruites par la plateforme des interceptions judiciaires. Le gouvernement s'engage à offrir des garanties techniques pour la centralisation, qui correspondent à un engagement financier de deux à quatre millions d'investissements.[38] Enfin, pour certains députés, la technique de l'IMSI Catcher est incompatible avec la protection de certaines professions, avocats, magistrats, journalistes, parlementaires[39]. En effet, l'antenne relais factice constituée par l'IMSI catcher recueille les données de connexion de tous les terminaux situés dans une zone géographique prédéfinie. Il est donc impossible d'en exclure certaines données sous prétexte de protéger certaines personnalités en raison de leurs fonctions dans la société, comme le précise le député Alain Tournet[40] dans son amendement 135[41] : « *La spécificité des professions en cause, au regard notamment de l'indépendance et du secret professionnel, ne permet pas le recours à un tel dispositif, qui est attentatoire aux droits de la défense* ». Ces amendements sont rejetés, sans qu'une réelle solution à ce conflit soit évoquée.

2. D'autres amendements adoptés

Il s'agit d'abord de préciser les conditions d'autorisation du recours aux IMSI Catcher [42] : la décision d'autorisation est écrite et motivée, le dispositif est mis en œuvre pendant une durée limitée, un mois renouvelable une fois durant l'enquête préliminaire, deux mois renouvelables deux fois pendant l'information judiciaire. Un double encadrement judiciaire implique l'intervention d'un officier de police judiciaire qui établit un procès-verbal des opérations de recueil des données et les modalités de centralisation, de conservation, de destruction des données recueillies, fixées par un décret en Conseil d'État pris après avis motivé et publié de la CNIL. Les données sont recueillies par la plateforme nationale des interceptions judiciaires[43] ; elles sont détruites à l'expiration du délai de prescription de l'action publique. Les IMSI Catcher ont été abondamment discutés tant à l'époque de l'adoption de la loi sur le renseignement qu'à l'occasion de la loi qui nous occupe. Certains amendements, très nombreux au demeurant, ont été rejetés ; ils insistaient sur la dichotomie entre la technique des IMSI Catcher et les principes de base des libertés individuelles et collectives. Cette affirmation peut se concevoir, car l'indifférenciation des personnes physiques qui correspond à ce dispositif rend illusoires le respect de la vie privée et la protection des données à caractère personnel.

---

[36]Mais, dans le cadre de cet amendement, les procédures incidentes ne seraient pas frappées de nullité.

[37]N° 363, Assemblée nationale, première séance du 3 mars 2016

[38]Référé de la Cour des Comptes, 25 avril 2016

[39]Cf. amendement n° 135, Assemblée nationale, première séance du 3 mars 2016

[40]Alain Tournet, député du Calvados, Groupe Gauche républicaine et démocratique

[41]Assemblée nationale, Amendement n° 135, première séance du 3 mars 2016

[42]N° 362, Assemblée nationale, première séance du 3 mars 2016

[43]PNIJ *« Le dispositif sera applicable au 1er janvier 2017. La PNIJ concentrera les interceptions judiciaires et les données recueillies par l'usage de l'IMSI catcher, soit l'annuaire inversé* », Jean-Jacques Urvoas, garde des Sceaux, Assemblée nationale, première séance du 3 mars 2016

III – Un débat sur le droit au chiffrement

A) L'origine du débat

Un débat animé s'instaure sur les rapports entre les États-nations et les multinationales qui peuvent refuser le déchiffrement de leurs données. La question se pose de savoir si la suprématie des États-nations perdure face à des sociétés commerciales qui se placent en marge de la légalité.

Au cours des débats sur le projet de loi, une affaire a fait grand bruit aux États-Unis. Apple a refusé de coopérer avec la justice pour fournir une méthode permettant de déchiffrer les données d'un iPhone appartenant à l'un des auteurs de la tuerie de San Bernardino.

Apple s'est ainsi opposé à une demande du FBI dans une lettre ouverte du 16 février 2016 signée par Tim Cook, son PDG : « *Le FBI exige que nous construisions une nouvelle version de notre système d'exploitation, désactivant des fonctionnalités de sécurité très importantes, pour l'installer sur des iPhone récupérés dans le cadre d'une enquête. Si ce logiciel tombait entre les mauvaises mains, cette personne pourrait potentiellement ouvrir n'importe quel iPhone* ». Tim Cook assimile cette demande à la création d'une porte dérobée, une faille laissée volontairement ouverte afin de laisser le FBI accéder aux données des produits Apple. Pour lui, l'acceptation de la requête du FBI permettrait au logiciel d'être utilisé à d'autres occasions ou par d'autres pays et de porter atteinte aux données à caractère personnel de tous les utilisateurs d'iPhone dans le monde. Le FBI, lui, fait valoir qu'il s'agit simplement de développer un outil permettant de déverrouiller un seul téléphone. Le 19 février 2016, le département américain de la Justice dépose un recours devant une cour fédérale pour amener Apple à répondre favorablement à la demande du FBI. Les arguments présentés par Apple sont considérés comme les composantes d'une stratégie marketing. Apple fait valoir qu'elle avait proposé plusieurs solutions au FBI afin d'accéder aux données de l'iPhone sans ouvrir l'appareil. Le FBI se réfère à l'« *All Writs Act* », une loi américaine votée en 1789 qui donne à une cour fédérale *« tous les moyens nécessaires ou appropriés pour aider sa juridiction et en conformité avec les principes du droit* ». Le 29 février 2016, Apple reçoit le soutien d'un juge new-yorkais, qui considère que le FBI outrepasse ses prérogatives en demandant à l'entreprise de l'aider à débloquer un iPhone. Cette décision intervient dans le cadre d'une affaire de trafic de drogues. Néanmoins, elle est symbolique pour Apple, car elle condamne le recours à l'« *All Writs Act* » qui était aussi invoqué dans l'affaire new-yorkaise. De nombreuses multinationales américaines[44] appuient la position d'Apple, en signant un mémoire à destination de la justice, mais la justice américaine n'est pas à même de suivre de telles formes de raisonnement. Dans le même sens, en août 2015, le procureur de Paris, François Molins, a signé un texte qui souligne que les techniques de chiffrement mises en place par de grands opérateurs empêchaient la justice d'agir. Le débat sur la question est mondial.

B) Un débat législatif en France

Dans ce contexte, est déposé en France dans le projet de loi portant réforme du code de procédure pénale un amendement n° 221 qui tend à punir de façon dissuasive l'opérateur de téléphonie mobile, le fournisseur d'accès à Internet, le fabricant d'un outil de téléphonie ou d'informatique qui refuserait de collaborer si une personne engagée dans une information judiciaire refuse ladite collaboration. L'amendement n° 221 reprend implicitement les arguments du FBI. Une interdiction temporaire de

[44]Exemples : Amazon, Facebook, Google, Microsoft, Yahoo…

commercialisation, dans un contexte similaire à l'affaire Apple, est proposée : ce serait la seule façon d'influencer des entreprises dont la capitalisation boursière atteint plusieurs centaines de milliards de dollars. Cela éviterait l'institution de zones de non-droit. L'amendement ne concerne pas l'ensemble des portables, mais seulement ceux pour lesquels il convient d'accéder aux données parce que l'instruction l'exige ou que le procureur de la République établit une demande auprès du juge des libertés et de la détention.

Le rapporteur de la loi fait remarquer que des sanctions pénales sont déjà prévues. Il découle des articles 230-1 à 230-5 du code de procédure pénale que le procureur de la République et la juridiction d'instruction ou de jugement peuvent requérir toute personne morale ou physique en vue de procéder à la mise au clair des données informatiques saisies ou obtenues pendant l'enquête ou l'instruction, et qui a fait l'objet d'opérations de chiffrement. Si la peine encourue est supérieure ou égale à deux ans d'emprisonnement et si les nécessités de l'enquête ou de l'instruction l'exigent, ces personnes sont en mesure de prescrire le recours aux moyens de l'État soumis au secret de la défense nationale, soit le centre technique d'assistance de la direction générale de la sécurité intérieure[45]. De plus, le législateur a reconnu à l'officier de police judiciaire le pouvoir de requérir une personne qualifiée pour la mise au clair de données chiffrées, afin de faciliter la mise en œuvre de cette procédure et réduire les délais de traitement des demandes de chiffrement. Selon le rapporteur[46], l'amendement semble « *dépasser la rigueur nécessaire à la juste répression de ces non-volontés de coopération »*[47], et manquer, en fait, au principe de proportionnalité. Les messageries chiffrées et sécurisées se sont développées[48]. La décision d'Apple de ne pas coopérer avec la justice s'explique en grande partie par son souci de rendre son offre crédible et attractive auprès de ses clients. Une coopération internationale est souhaitable, mais n'exclut pas un effort législatif national. L'amendement n° 221 est mis aux voix. Sur les 24 votants, 23 sont des suffrages exprimés : 11 voix sont pour l'adoption, 12 voix sont contre. L'amendement n'est donc pas adopté, mais a donné lieu à de nombreuses discussions, notamment sur l'influence de l'armée américaine dans la conception des réseaux chiffrés au niveau communautaire et international. Cette affaire n'a pour l'instant débouché sur aucune norme française, mais le débat n'est pas clos, et les divers intérêts en présence, économiques, juridiques sont toujours en opposition. Le 4 mars 2016, le haut-commissaire de l'ONU aux droits de l'Homme estime que la décision de forcer Apple à se plier aux ordres du FBI risquerait « *d'ouvrir une boîte de Pandore avec des implications qui pourraient être extrêmement dommageables pour les droits de l'Homme de millions de personnes, y compris pour leur sécurité physique et financière* ». Cette opinion n'est pas convaincante : les multinationales sont guidées par le souci de réaliser des profits, non pas en premier lieu par la préoccupation de faire respecter les droits de l'homme. Alors que le « *Safe Arbor Principles* » a été invalidé par la Cour de justice de l'Union européenne[49] et que le nouveau règlement européen[50] sur les données à caractère personnel, très différent de l'autorégulation américaine, est entré en vigueur, les débats sur la façon de concevoir les données à caractère personnel et les façons de les protéger sont loin d'être clos.

[45]La DGSI

[46]Pascal Popelin

[47]Assemblée nationale, première séance du 3 mars 2016

[48]Telles que Huawei en Chine ou Telegram

[49]Décision du 6 octobre 2015

[50]Règlement 2016/679 du 26 avril 2016

IV – De la biométrie

La loi du 3 juin 2016 s'intéresse aussi à la biométrie[51], dans le cadre du Chapitre IV de la loi, et aux dispositions relatives à la défense. Dans l'article 116, le livre III de la deuxième partie du code de la défense est complété par un titre VIII ainsi dénommé « *De la biométrie*. ». Lors d'une opération mobilisant des capacités militaires se déroulant à l'extérieur du territoire français, les membres des forces armées et formations rattachées sont susceptibles de procéder à des opérations de relevés signalétiques, pour établir l'identité, lorsqu'elle est inconnue ou incertaine, et la participation antérieure aux hostilités des personnes décédées lors d'actions de combat et de personnes capturées par les forces armées. En vue de finalités identiques, les membres des forces armées sont habilités à réaliser des prélèvements biologiques destinés à permettre l'identification de l'empreinte génétique de ces personnes.

Les données ayant fait l'objet d'une collecte peuvent être consultées dans le cadre d'enquêtes préalables à une décision de recrutement ou d'accès à une zone protégée arrêtée par l'autorité militaire. C'est un décret en Conseil d'État qui fixe la liste des enquêtes qui donnent lieu à la consultation et les modalités d'information des personnes concernées.

V – La jurisprudence : état d'urgence, sécurité et ordre public

La loi du 21 juillet 2016 proroge une nouvelle fois l'état d'urgence régi par la loi n° 55-385 du 3 avril 1955 modifiée et apporte de nouveaux éléments de luttes et de garanties relatives au terrorisme. Une première jurisprudence du Conseil d'État du 5 août 2016 illustre les pouvoirs respectifs dévolus au préfet et au juge administratif concernant l'autorisation d'exploiter des données contenues dans un téléphone portable saisi lors d'une perquisition administrative effectuée le 29 juillet 2016.

Les faits : le préfet du Var demande au juge des référés du tribunal administratif de Toulon, en se fondant sur l'article onze de la loi du 3 avril 1955 d'autoriser l'exploitation des données contenues dans le téléphone portable de M. A. saisi lors d'une perquisition administrative réalisée le 29 juillet 2016 à son domicile. Par une ordonnance en date du 2 août 2016, le juge des référés du tribunal administratif de Toulon rejette la demande. Par une requête enregistrée le 4 août 2016 au secrétariat du contentieux du Conseil d'État, le ministère de l'Intérieur demande au juge des référés du Conseil d'État statuant sur le fondement de l'article onze de la loi du 3 avril 1955 d'annuler l'ordonnance, de donner suite à la demande de première instance. L'ordonnance serait entachée d'une erreur de droit[52] et d'une erreur d'appréciation. Une audience publique est organisée, en présence du ministère de l'Intérieur et de M. A. Le droit : aux termes de l'article premier de la loi du 21 juillet 2016, l'état d'urgence est prorogé pour une durée de six mois. La perquisition[53] permet d'accéder à des données stockées dans le système ou un équipement ou dans un autre système informatique, dans la mesure où les données sont accessibles à partir du système initial ou disponibles pour le

[51] Article 116

[52] Le juge des référés a considéré qu'il ne lui revenait pas d'examiner la légalité de l'opération de perquisition dans son ensemble et a estimé qu'il devait se prononcer sur la réalité de la menace que pouvait constituer M. A. et qui avait justifié la décision de perquisition

[53] Selon le I de l'article onze de la loi n° 55-385 du 3 avril 1955, l'autorité administrative peut ordonner une perquisition à condition que ladite perquisition soit régularisée dans « les meilleurs délais » et que le Procureur de la République soit informé

système initial. Lorsque la perquisition permet de déterminer l'existence d'éléments, notamment informatiques, afférents à la menace constituée pour la sécurité et l'ordre public par une certaine personne, les données concernées sont susceptibles d'être saisies par leur copie, leur support. La copie est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition procède à un procès-verbal. L'autorité administrative sollicite du juge des référés, dès la fin de la perquisition, l'autorisation d'exploitation. Ce juge statue dans les quarante-huit heures. En cas de refus du juge des référés, un appel est possible. Ensuite, les données copiées sont détruites et les supports restitués à leur propriétaire. À la suite de l'ordre de perquisition pris par le préfet du Var le 28 juillet 2016, la perquisition s'est déroulée en présence d'un officier de police judiciaire compétent ainsi que de M. A. À l'issue de la perquisition, le procureur de la République a été immédiatement informé. La procédure de saisie du téléphone portable est donc régulière.

Par ailleurs, le ministre de l'Intérieur a fait valoir que l'examen sommaire de l'appareil a révélé qu'il contenait des vidéos salafistes, qui pourraient témoigner d'une pratique radicalisée de la religion musulmane par l'intéressé et aussi des contacts, via un réseau social, avec des individus vivant en zone de combat syro-irakienne. Le procès-verbal du 29 juillet et la demande du préfet ne mentionnent pas ce point, mais le ministre argue qu'il s'agit d'une simple omission, que le rapport de saisie du 31 juillet établi par l'officier de police mentionne cet élément. Au cours de la perquisition, M. A. a admis que l'un de ses frères était mort en Irak en 2014 à la suite d'un attentat suicide. Le ministre produit devant le Conseil d'État une note faisant état des liens entretenus par M. A. qui s'est rendu en Allemagne pendant l'été 2015 avec un ressortissant allemand impliqué dans plusieurs projets d'attentats en Allemagne, parti en Syrie rejoindre les rangs de l'« État islamique » et faisant l'objet d'un mandat d'arrêt international pour association de malfaiteurs en relation avec une entreprise terroriste. Dans ce contexte, le téléphone portable saisi est susceptible de contenir des données relatives à la menace que constitue M. A pour la sécurité et l'ordre public.

L'autorité administrative est donc autorisée à exploiter les données contenues dans le téléphone portable de M. A. L'ordonnance du juge des référés du tribunal administratif de Toulon en date du 2 août 2016 est annulée.

Conclusion

Plus que la nouvelle répartition entre Parquet, juge d'instruction, juge des libertés et de la détention, la loi du 3 juin 2016, pour ce qui concerne le numérique et les communications électroniques, élargit le champ d'application possible du contrôle des personnes. Comme cette loi vient compléter la loi antiterroriste et la loi sur le renseignement, l'exécutif a à sa disposition un grand éventail de moyens pour diligenter la surveillance des personnes physiques. Les mesures prévues ne semblent pas en mesure de garantir les libertés individuelles et collectives, malgré les efforts du législateur. En dépit des proclamations d'intention du Conseil d'État dans son avis, qui souhaitait parvenir à un équilibre entre sécurité et liberté, dans le seul domaine des communications électroniques, la balance penche presque exclusivement en faveur de la sécurité : les durées, même si elles sont provisoires par définition sont trop longues au regard des libertés individuelles. Surtout, les IMSI Catcher, de par leur caractère indistinct peuvent capter non seulement des données de connexion, mais parfois du contenu, et ceci, sur un périmètre géographique qui peut être vaste, et sans pouvoir « *protéger* » les personnes, qui, de par leur immixtion obligée dans l'existence des personnes physiques, participent à la vie privée des individus. Les caméras mobiles, qui ont longtemps été au stade de l'expérimentation

n'apporteront peut-être pas tous les bienfaits escomptés par cette réforme. Il est probable que le contrôle lors des opérations de police ou de gendarmerie pose des problèmes, dont la plupart ne sont pas encore perceptibles. La Plateforme nationale des interceptions judiciaires va naître juridiquement dans de multiples incertitudes. La mutualisation des interceptions judiciaires et administratives portera-t-elle ses fruits ? Les opérations ne feront plus l'objet d'un paiement à l'acte. La Cour des comptes[54] insiste sur la nécessité de respecter *« les principes d'indépendance de la justice, de primauté de l'autorité judiciaire, de secret de l'enquête et de l'instruction ainsi que sur la protection du secret de la défense nationale* ». Ces principes sauront-ils s'imposer ? La captation des données informatiques à distance, des images et des sons parviendra-t-elle à faire cohabiter efficacité et maintien des libertés ? Tout cela reste incertain.

Par ailleurs, cette loi s'agrège à des lois antérieures qui avaient déjà diminué le champ d'application du domaine réservé au respect de la vie privée et à la protection des données à caractère personnel.

La situation géopolitique, avec un seul organisme militaire de dimension mondiale[55], une seule puissance militaire mondiale susceptible d'intervenir sur tous les théâtres d'opérations, les États-Unis, la perpétuation vraisemblable des actes de terrorisme et de l'exploitation médiatique qui en est faite constamment, ce qui amène à justifier, pour de nombreux élites ou groupes politiques, de nouvelles constructions sécuritaires passant par l'innovation technologique et le numérique, tout cela laisse peu de place à la pérennité d'un espace de liberté. La loi du 3 juin 2016 continue ce mouvement vers ce panoptique qui semble chaque jour un peu plus réel. Les contre-pouvoirs ne sont pas inexistants. Pendant l'adoption de la loi du 3 juin 2016, la plupart des organisations de défense des libertés publiques, telles que le Syndicat de la magistrature ou le Syndicat des Avocats de France, ont fait connaître leurs analyses et leurs réticences. Il en est de même pour les organismes spécialisés dans le numérique et l'Internet, comme « *La Quadrature du Net* », mais ces contre-pouvoirs ont surtout des outils symboliques.

La CNIL, via les avis qui accompagneront les nombreux décrets en Conseil d'État prévus par cette loi, serait, dans une certaine mesure, apte à infléchir certains articles des futurs décrets. Cependant, bien qu'elle soit une autorité administrative indépendante reconnue et appréciée, la CNIL n'a ni les moyens ni la volonté de s'opposer aux possibles velléités sécuritaires de l'exécutif : cela ne correspond ni à ses attributions ni à ses missions.

Dans ce contexte, les procédures de contrôle social croissent de façon exponentielle, et les citoyens sont isolés. C'est pourquoi il est possible de s'interroger, avec Julie Alix : *« Dans sa volonté d'appréhender le phénomène terroriste, le droit pénal s'expose donc à un double risque : devenir un droit inefficace ou un droit liberticide »*[56] *et « Quel degré de violence la démocratie peut-elle mettre en œuvre pour combattre le terrorisme ? Telle est par conséquent la question que pose aujourd'hui la lutte contre le terrorisme. Appliquée au droit pénal, cette interrogation générale se décline ainsi : comment, à l'épreuve des plus graves criminalités collectives, le droit pénal peut-il rester démocratique ? ».*

[54]Cité par Marc Rees « *PNIJ quand la Cour des comptes étrille les choix du gouvernement* », NextINpact, 25 avril 2016

[55]L'OTAN

[56]Julie Alix, « *Terrorisme et droit pénal* », Paris, Dalloz, 2010, p. 10