

LES DIFFÉRENTES FORMES D'INFILTRATION DES GROUPES CRIMINELS EN TANT QUE PROCÉDÉS D'INVESTIGATION EN DROIT FRANÇAIS ET QATARIEN

Professeur\ Magdy Habchy

Maître de Conférences Habilité à Diriger des Recherches

Faculté de Droit et de Sciences Politiques - Université de Reims – Champagne Ardenne

LES DIFFÉRENTES FORMES D'INFILTRATION DES GROUPES CRIMINELS EN TANT QUE PROCÉDÉS D'INVESTIGATION EN DROIT FRANÇAIS ET QATARIEN

Professeur\ Magdy HABCHY

Maître de Conférences Habilité à Diriger des Recherches

Faculté de Droit et de Sciences Politiques - Université de Reims – Champagne Ardenne

RÉSUMÉ

Cette étude vise à proposer au législateur qatari un modèle législatif intégré relatif à l'utilisation des moyens procéduraux et des technologies modernes dans la lutte contre la criminalité organisée et la cybercriminalité, à la lumière des applications jurisprudentielles ainsi que des difficultés susceptibles d'être soulevées par la pratique, notamment la problématique de la conciliation entre les nécessités de l'enquête et la protection des droits de la défense.

Il convient, à cet égard, de distinguer entre la notion d'infiltration des groupes criminels en tant que mécanisme procédural complet destiné à faire face aux crimes graves et organisés, et celle de la force probante de la preuve électronique, laquelle demeure limitée aux infractions informatiques. Dès lors, cette étude distingue deux formes d'infiltration des organisations criminelles : d'une part, l'infiltration directe, qui suppose que les auteurs aient connaissance de cette intervention, croyant que l'enquêteur n'est qu'un complice ou une victime potentielle ; d'autre part, l'infiltration indirecte ou clandestine, dont le succès repose essentiellement sur l'ignorance des auteurs quant à son existence.

L'étude met également en évidence que le législateur français a défini le cadre juridique de la légalité des différentes formes d'infiltration et d'intrusion, en limitant ces procédures au domaine de la criminalité organisée et en confiant le pouvoir d'en autoriser l'exécution au juge d'instruction en cas d'ouverture d'une information judiciaire, ainsi qu'au juge des libertés et de la détention dans le cadre d'une enquête policière. Le législateur a par ailleurs soumis ces mesures à des conditions de fond et de forme, dont la violation entraîne la nullité de la procédure.

Mots-clés: Les groupes criminels, La criminalité organisée, La force probante de la preuve électronique.

المُلخَص

الأوجه المختلفة لاختراق الجماعات الإجرامية كوسيلة إجرائية للاستدلال والتحقيق في القانون الفرنسي والقطري

الأستاذ الدكتور/ مجدي أنور حبشي

أستاذ محاضر (إجازة الاشراف على رسائل الدكتوراه) متفرغ بقسم القانون الخاص والعلوم الجنائية
كلية الحقوق والعلوم السياسية بجامعة رنس - عضو الدفاع امام المحكمة الجنائية الدولية

تهدف هذه الدراسة إلى أن تضع أمام المشرع القطري نموذجاً تشريعياً متكاملًا، فيما يتعلق باستخدام الوسائل الاجرائية والتقنيات الحديثة لمكافحة الجريمة المنظمة والالكترونية، في ضوء التطبيقات القضائية، وما قد يثيره التطبيق العملي من مشكلات، لاسيما إشكالية التوفيق بين ضرورات التحقيق وحماية حقوق الدفاع. حيث يتعين التفرقة بين فكرة اختراق الجماعات الاجرامية، كتنظيم اجرائي متكامل لمجابهة الجرائم الجسيمة والمنظمة، وبين فكرة حجية الدليل الالكتروني، الذي يقتصر على الجرائم الالكترونية. وعلى ذلك تم تقسيم هذه الدراسة الى نوعين من الاختراق للجماعات الاجرامية، وهما على هذا النحو: الاختراق المباشر من ناحية أولى، والذي يفترض علم الجناة بهذا التداخل اعتقاداً منهم بأن المحقق مجرد شريك أو مجني عليه محتمل، والاختراق غير المباشر أو المستتر، والذي يفترض كشرط أساسي لنجاح عملية الاختراق، عدم علم الجناة بها.

وقد بدا واضحاً في هذه الدراسة أن المشرع الفرنسي قد حدد الإطار القانوني لمشروعية كافة صور الاختراق والتسلل، والذي بمقتضاه حصر هذه الإجراءات في إطار الجرائم المنظمة وأولى سلطة الامر بها إلى قاضي التحقيق، - حال فتح تحقيق قضائي- وقاضي الحريات حال فتح تحقيق بوليسي. وقد أخضع المشرع هذه الإجراءات لشروط موضوعية وشكلية، يترتب على مخالفتها بطلان الاجراء.

الكلمات المفتاحية: الجماعات الإجرامية ، الجريمة المنظمة ، حجية الدليل الالكتروني

Introduction

Face à la sophistication croissante de la criminalité organisée, notamment dans les domaines du trafic des stupéfiants, du terrorisme ou encore de la cybercriminalité¹, le législateur a dû renforcer les techniques d'enquête en utilisant des moyens plus adaptés. Parmi ceux-ci, l'infiltration occupe une place singulière. Technique d'investigation exceptionnelle, elle consiste, pour un officier ou agent de police judiciaire dûment habilité, à agir sous une identité d'emprunt, afin de s'intégrer dans un groupe criminel pour observer, recueillir des preuves ou participer à des transactions illicites contrôlées.

C'est dans cette perspective que la loi du 9 mars 2004², complétée par la loi du 19 novembre 2019, a inséré au code de procédure pénale de nouveaux actes d'administration de la preuve, y compris l'infiltration³, pour le recueil des indices nécessaire à la constatation des infractions qu'elle a limitativement énumérées comme entrant dans le champ d'application des articles 706-73, 706-73-1 ou 706-74. Ce dispositif a été complété par les lois du 23 mars et 18 septembre 2019⁴.

Ces modes de preuve qui peuvent être utilisés exclusivement dans le cadre de la criminalité organisée ont été complétés par des procédés propres pour lutter contre la cybercriminalité de droit commun. En effet, les cybers délinquants, en utilisant la dématérialisation des échanges, peuvent commettre leurs infractions à l'abri du regard des autorités policières et, à ce titre, ils profitent de l'anonymat renforcé que procure Internet pour échanger de façon anonyme.

Aussi, le législateur est intervenu plusieurs fois pour prévoir des procédés spécifiques destinés à permettre aux enquêteurs spécialisés d'infiltrer les filières de criminalité organisée. Ce dispositif permet aux autorités policières de participer activement à l'infraction en introduisant un de leurs agents dans le groupe criminel, en se faisant passer pour un membre du réseau.

(1) Il faut distinguer la criminalité numérique de la criminalité organisée. Tandis que la criminalité numérique désigne toute forme cybercriminalité de droit commun, la criminalité organisée s'étend aux crimes et délits graves entrant dans le champ d'application des articles 706-73, 706-73-1 ou 706-74, du code de procédure pénale.

(2) Le cadre d'enquête coercitif ajouté, propre à la criminalité organisée, a été créé par la loi du 9 mars 2004.

(3) Ce procédé a été reconnu par des conventions internationales. C. des Nations Unies contre la criminalité transnationale organisée, du 12 sept. 2000, (art. 20), entré en vigueur le 29 septembre 2003 – C. de Vienne, du 20 déc. 1988, contre le trafic illicite de stupéfiants et des substances psychotropes, art. 11.

(4) Sur une étude de la loi du 23 mars 2019 : MAYAUD, De la loi au Conseil constitutionnel, une réforme contrastée de la procédure pénale, AJP 2019. 176. – PRADEL, Notre procédure pénale à la recherche d'une efficacité à toute vapeur. Loi no 2019-222 du 23 mars 2019, JCP 2019. Étude 406

A ce procédé d'infiltration propre à la criminalité organisée⁵ s'ajoute l'enquête sous pseudonyme sur les réseaux numériques appelée également l'infiltration numérique, qui est prévue par l'article 230-46 du code de procédure pénale. Selon ce texte « aux seules fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques » les officiers ou agents de police judiciaire habilités peuvent commettre les différents actes de l'infiltration numérique.

Il en résulte que le législateur prévoit deux formes d'infiltration directe soumises à des conditions différentes. L'infiltration numérique de droit commun et l'infiltration physique en matière de criminalité organisée⁶. A ces deux formes d'investigation s'ajoutent différentes formes d'infiltration indirecte, à travers des procédés d'interception, d'accès à distance aux correspondances stockées dans un système informatique, ou de captation des données numériques propres à la criminalité organisée.

Problématique de l'étude

L'étude de ces moyens d'investigation nous amène à nous interroger, dans quelle mesure l'infiltration et les autres procédés constituent-ils des modes d'investigation efficaces tout en demeurant compatibles avec les principes directeurs de la procédure pénale ?

En effet, ces différentes techniques d'enquête, qui impliquent une immersion prolongée dans des milieux délinquants et parfois la participation apparente à des activités illicites, soulèvent des enjeux juridiques majeurs.

Encadrée strictement par le code de procédure pénale⁷ ce procédé doit concilier efficacité répressive et respect des libertés fondamentales.

Ainsi, dans la mesure où l'infiltration constitue un outil d'exception dont la mise en œuvre requiert un équilibre délicat entre nécessités opérationnelles et garanties procédurales, il revient alors au législateur de trouver cet équilibre. C'est dans ce cadre, que cette étude a pour objet d'examiner principalement le système mis

(5) Le conseil constitutionnel a considéré que la notion de bande organisée qui constitue un des critères de la criminalité organisée « n'est ni obscure, ni ambiguë et se distingue ainsi de la notion de réunion et de coaction » (Décis. 2 mars 2004, no 2004-492 DC).

(6) Il est évident que l'infiltration physique qui s'applique en matière de criminalité organisée peut être accompagnée d'une infiltration numérique du droit commun.

(7) Sans oublier le rôle de la jurisprudence, v sur Le principe de loyauté de la preuve, cour de cassation - Assemblée plénière — 9 décembre 2019 - n° 18-86.767

en place par le législateur français afin de trouver ce point d'équilibre entre ces exigences contradictoires⁸.

Sans pouvoir faire une étude comparée approfondie avec le droit qatarien, compte tenu de la diversité des approches, nous signalons à la fin de chaque développement du droit français les dispositions prévues par le législateur qatarien.

Plan

L'examen des différentes techniques d'enquête ou d'instruction, qui impliquent une immersion prolongée dans des milieux délinquants, montre la multiplicité de ces techniques d'infiltration des groupes criminels.

A la forme spécifique de l'infiltration numérique destinée à lutter contre les infractions du droit commun commises par la voie des communications électroniques, s'ajoute, tout en s'en distinguant, l'infiltration en général, admise en matière de criminalité organisée d'une part, et les différentes formes d'immersion, d'interception ou de captation des communications électroniques ou des données informatiques qui peuvent être mises en place en vertu des techniques spéciales d'enquête et qui sont prévues en matière de criminalité organisée, d'autre part.

Au-delà de cette énumération, ces différents actes d'investigation constituent, en réalité, soit une mesure d'infiltration directe (chapitre 1) qui implique l'entrée en contact avec les auteurs ou complices, soit une infiltration indirecte des groupes criminels (chapitre 2) qui se fait à travers des procédés dissimulés.

(8) CEDH, 8 février 2018, AFFAIRE BEN FAIZA c. France (Requête n° 31446/12).

Chapitre 1.- L'infiltration directe

L'infiltration directe est une forme d'infiltration trompeusement affichée, en ce sens que la présence de l'agent infiltré est connue de l'auteur de l'infraction, pris faussement pour une victime potentielle ou un complice.

Sous ce vocable, nous abordons donc deux formes d'infiltration de natures différentes, qui sont par conséquent soumises chacune à un régime autonome, à savoir, d'une part, la forme spécifique de l'infiltration numérique, qui s'applique aux infractions du droit commun commises par la voie des communications électroniques, laquelle constitue une forme d'infiltration virtuelle (section 1), et d'autre part, l'infiltration physique, admise en matière de criminalité organisée (section 2).

Section 1. L'infiltration numérique propre aux infractions commises par voie de communications électroniques

L'infiltration numérique appelée par le législateur l'enquête sous pseudonyme consiste à autoriser certains policiers spécialement habilités à procéder, sous pseudonyme, à infiltrer les réseaux numériques et à accomplir certains actes sans en être pénalement responsables. Ce procédé peut être utilisé aux seules fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques.

Nous précisons la notion de l'infiltration numérique (sous-section1) avant d'indiquer les conditions requises pour recourir à ce procédé (sous-section 2).

Sous-section 1. La notion d'infiltration numérique

L'infiltration numérique constitue un moyen d'investigation destiné à lutter contre la criminalité numérique, ayant pour objet d'autoriser les enquêteurs à participer sous un pseudonyme aux échanges électroniques ou à extraire des données informatiques constituant des crimes ou délits punis de la peine d'emprisonnement. Pour renforcer l'efficacité de ce procédé, le législateur est intervenu récemment⁹ pour autoriser les enquêteurs à faire usage d'un dispositif permettant d'altérer ou de transformer leur voix ou leur apparence physique.

Ainsi définie, l'infiltration numérique doit être distinguée de l'infiltration en matière de criminalité organisée, d'une part, et de l'anonymisation procédurale de l'article 15-4 du code de procédure pénale, d'autre part.

(9) LOI n°2025-532 du 13 juin 2025, ayant modifié l'article 230-46 du code de procédure pénale

I. La distinction entre l'infiltration numérique et l'infiltration propre à la criminalité organisée

L'infiltration numérique se distingue doublement de l'infiltration propre à la criminalité organisée.

Tout d'abord, outre sa forme numérique destinée à lutter contre la criminalité numérique, l'infiltration numérique est plus souple que les opérations d'infiltration de la criminalité organisée¹⁰. Tandis que l'infiltration numérique est un moyen d'investigation du droit commun qui s'applique aux crimes et délits, punis d'une peine d'emprisonnement, commis par la voie des communications électroniques, l'infiltration en matière de criminalité organisée implique la constatation d'un crime ou de délits faisant partie de la liste de cette catégorie d'infraction.

Ensuite, contrairement à l'infiltration numérique qui a pour objet d'autoriser des policiers habilités à participer sous un pseudonyme aux échanges électroniques et à se trouver en contact avec les personnes susceptibles d'être les auteurs ou complices d'infractions dans le but de rassembler la preuve numérique de ces infractions, l'infiltration en matière de criminalité organisée implique que l'agent infiltré entre en contact physique avec une personne suspecte, en se faisant passer pour un participant à la réalisation de l'infraction.

II. La distinction entre l'infiltration numérique et l'anonymisation procédurale de l'article 15-4

Cette distinction est nécessaire dans la mesure où le législateur utilise les termes « enquête sous pseudonyme » pour désigner l'infiltration numérique.

L'anonymisation est un procédé qui permet à tout agent, dans l'exercice de ses fonctions, d'être autorisé à ne pas être identifié par son nom et prénom dans les actes de procédure, lorsque la révélation de son identité est susceptible de mettre en danger sa vie ou son intégrité physique ou celle de ses proches, compte tenu des conditions d'exercice de sa mission ou de la nature des faits qu'il est habituellement amené à constater.

L'agent visé est tout agent de la police nationale ou de la gendarmerie nationale, ainsi que certains agents des douanes et des services fiscaux mentionnés aux articles 281, 28-1-1 et 28-2.

(10) M. Quémener « Infiltrations numériques et enquêtes sous pseudonyme », Juris Classeur Communication, Fasc. 1110.

a. Conditions de l'anonymisation

Ce procédé d'anonymisation peut être autorisé dans deux cas.

D'une part, lorsque les procédures portent sur un crime ou un délit puni d'au moins trois ans d'emprisonnement, et d'autre part, dans les autres cas, lorsque la révélation de l'identité de l'agent est susceptible de mettre en danger sa vie ou son intégrité physique ou celles de ses proches, en raison de circonstances particulières de la commission des faits ou de la personnalité des personnes mises en cause.

L'autorisation est délivrée nominativement par un responsable hiérarchique d'un niveau suffisant, défini par décret, statuant par une décision motivée. Copie en est transmise au Procureur de la République territorialement compétent.

b. Effets de l'anonymisation

Le bénéficiaire de l'autorisation est en principe autorisé à déposer ou à comparaître comme témoin au cours de l'enquête ou devant les juridictions d'instruction ou de jugement et à se constituer partie civile en utilisant ces mêmes éléments d'identification, qui sont seuls mentionnés dans les procès-verbaux, citations, convocations, ordonnances, jugements ou arrêts. Il ne peut être fait état de ses nom et prénom au cours des audiences publiques.

Mais les juridictions d'instruction ou de jugement saisies des faits ont accès aux nom et prénom de la personne identifiée par un numéro d'immatriculation administrative dans un acte de procédure.

c. Contestation de l'anonymisation

Le juge d'instruction ou le président de la juridiction de jugement peuvent être saisis par une partie à la procédure d'une requête écrite et motivée tendant à la communication des nom et prénom de l'agent.

Après avis du ministère public, la juridiction décide des suites à donner à cette requête en tenant compte, d'une part, de la menace que la révélation de l'identité de cette personne ferait peser sur sa vie ou son intégrité physique ou celles de ses proches et, d'autre part, de la nécessité de communiquer cette identité pour l'exercice des droits de la défense de l'auteur de la demande. Par ailleurs, cette anonymisation ne fait pas obstacle à toute demande en nullité. Dans cette situation le juge d'instruction, le président de la chambre de l'instruction ou le

président de la juridiction de jugement statue sur cette nullité. Toutefois, cet examen doit respecter l'anonymisation au cours du débat contradictoire et dans sa décision.

d. Sanction de la violation de l'anonymisation

Sauf décision du juge ou du président de la juridiction de lever l'anonymat, est constitutif d'un délit puni de cinq ans d'emprisonnement et de 75 000 € d'amende, la révélation des nom et prénom de l'agent bénéficiaire, ou de tout élément permettant son identification personnelle ou sa localisation. Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende, lorsque cette révélation a entraîné des violences à l'encontre du bénéficiaire de l'autorisation ou de son conjoint, de ses enfants ou de ses ascendants directs, et les peines sont portées à dix ans d'emprisonnement et à 150 000 € d'amende, lorsque cette révélation a entraîné la mort des personnes mentionnées.

Sous-section 2. Les conditions de l'infiltration numérique

L'infiltration numérique est subordonnée à l'existence de certaines conditions de forme et de fond, afin de pouvoir autoriser l'accomplissement de certains actes.

I. Les conditions de la mise en place de l'infiltration numérique

a. Les conditions de forme

En premier lieu, l'infiltration est réservée aux officiers ou agents de la police judiciaire, affectés dans un service spécialisé et spécialement habilités, à cette fin, par arrêté du ministre de la justice et du ministre de l'intérieur.

En deuxième lieu, certains actes nécessitent une autorisation du procureur de la république, en cas d'enquête, et du juge d'instruction en cas d'information. Cette autorisation, qui peut être donnée par tout moyen, est mentionnée ou versée au dossier de la procédure. Le non-respect de cette règle est sanctionné par une nullité textuelle.

En troisième lieu, l'infiltration numérique et les actes qui en découlent s'effectuent, selon le cas, sous le contrôle du Procureur de la République, en cas d'enquête, ou du juge d'instruction, en cas d'instruction préparatoire.

b. Les conditions de fond

En premier lieu, l'infiltration numérique doit être mise en place aux seules fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques. Il en résulte que si ce procédé peut être mis en place pour constater des infractions du droit commun, c'est à la double condition que l'infraction soit commise par voie des communications électroniques et qu'elle soit punie d'une peine d'emprisonnement. Il en résulte que ce procédé ne peut pas être utilisé si le délit est puni d'une peine d'amende seulement.

En second lieu, soumis au principe de loyauté¹¹, les actes accomplis ne peuvent pas constituer une incitation à commettre une infraction. Bien que ce principe soit prévu par l'avant dernier alinéa de l'article 230-46 en ce qui concerne seulement les actes soumis à une autorisation judiciaire qui sont prévus aux 3° et 4° paragraphes de ce texte, il va de soi que l'ensemble de l'infiltration numérique doit respecter le principe de loyauté¹².

Par ailleurs, le législateur est intervenu très récemment¹³ pour délimiter la définition de la notion d'incitation à commettre une infraction. Selon la nouvelle formulation « ne constituent pas une incitation à commettre une infraction les actes qui contribuent à la poursuite d'une infraction déjà préparée ou débutée au moment où l'autorisation mentionnée au présent article a été accordée par le magistrat compétent, y compris en cas de réitération ou d'aggravation de l'infraction initiale ». Il en résulte que le législateur utilise le critère de la commission préalable de l'infraction pour déterminer s'il a y ou non une incitation à commettre l'infraction. Ce critère doit englober en toute logique la commission des actes constituant un simple commencement d'exécution, même si l'infraction consommée n'a pas été accomplie.

II. Les actes autorisés

L'article 230-46 prévoit quatre catégories d'actes qui peuvent être classés en deux catégories, selon l'exigence ou non d'une autorisation judiciaire.

a. Les actes qui peuvent être accomplis sans autorisation judiciaire

Il s'agit d'abord des actes de constatation passive, tel le fait de participer à des échanges électroniques, y compris avec les personnes susceptibles d'être les

(11) A. Lepage, « La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet » : Comm. com. électr. 2014, comm. 73

(12) M. Quémener : « Infiltrations numériques et enquêtes sous pseudonyme », JurisClasseur Communication, Fasc. 1110

(13) LOI n°2025-532 du 13 juin 2025, ayant modifié l'article 230-46 du code de procédure pénale

auteurs de ces infractions, et par conséquent, le fait d'extraire ou de conserver par ce moyen les données sur les personnes susceptibles d'être les auteurs de ces infractions, et tout élément de preuve¹⁴.

C'est par application de ces dispositions que la jurisprudence a rendu certaines décisions ayant admis le recours à l'infiltration numérique. Tel est le cas de l'arrêt rendu par la chambre criminelle le 25 janvier 2023¹⁵. En l'espèce, en janvier 2021, un individu est entré en relation, sur un site internet, avec un enquêteur en charge d'une opération de cyber-infiltration tendant à lutter contre la pédophilie en ligne et se faisant passer pour une fillette âgée de 12 ans. A la suite de cet échange, le prévenu s'est rendu le 2 février 2021 en voiture sur le lieu de rendez-vous qu'il avait fixé en ligne, avec son interlocuteur en vue d'avoir une relation sexuelle, et il a été interpellé. La cour de cassation a confirmé la régularité de ce procédé et la condamnation de cet individu en vertu de l'article 227-22-1 du code pénal, qui vise les propositions sexuelles à un mineur de quinze ans en utilisant un moyen de communication électronique¹⁶.

b. Les actes soumis à une autorisation judiciaire

Cette autorisation est accordée par le procureur en cas d'enquête et par le juge d'instruction en cas d'information.

Il s'agit des actes intrusifs et actifs, qui impliquent la commission des actes normalement infractionnels. Le texte vise deux catégories d'actes.

Tout d'abord, le fait d'acquérir tout contenu, produit, substance, prélèvement ou service ou de les transmettre en réponse à une demande expresse.

Ensuite, le fait d'acquérir, de transmettre ou de vendre, par les personnes susceptibles d'être les auteurs de ces infractions, tout contenu, produit, substance, prélèvement ou service, y compris illicite d'une part, et le fait de mettre à la disposition des personnes susceptibles d'être les auteurs de ces infractions, des moyens juridiques ou financiers ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication, d'autre part.

(14) Éric A. Caprioli et P. Agosti, « La confiance dans l'économie numérique. Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique » : LPA 3 juin 2005, n° 110,

(15) Crim. 25 janvier 2023, 22-83.997

(16) A. Plantevin, « Les propositions sexuelles faites à un mineur de quinze ans par un moyen de communication électronique » : Gaz. Pal. 27 oct. 2012, n° 301, p. 24 A.-G. Robert « Délit de propositions sexuelles faites à un mineur de quinze ans par un moyen de communication électronique » : RSC 2008, chron. p. 867

Sous-section 3. L'infiltration numérique en droit qatarien

Il convient d'exposer les différents textes qui prévoient l'infiltration numérique en droit qatarien, avant d'en préciser le régime.

I. Les différentes manifestations d'infiltration numérique en droit qatarien

La loi n° (14) de 2014 relative à la lutte contre la cybercriminalité prévoit certaines règles concernant la preuve numérique. Il en est ainsi de l'article 17 de cette loi qui prévoit que « Le ministère public peut ordonner la collecte et l'enregistrement immédiats de toutes les données ou informations électroniques, données de trafic ou informations de contenu qu'il juge nécessaires aux fins de l'enquête ». Il en résulte que la collecte ou l'enregistrement peuvent être accomplis à la suite d'une infiltration numérique.

Par ailleurs, l'article 16 de cette loi prévoit qu'« aucun élément de preuve obtenu par l'autorité compétente ou les autorités chargées de l'enquête d'autres États ne peut être écarté pour cette seule raison, dès lors qu'il a été obtenu conformément aux procédures légales et judiciaires de coopération internationale ». Il en résulte que les preuves obtenues légalement à l'étranger par des autorités étrangères à la suite d'une mesure d'infiltration numérique peuvent être invoquées devant la juridiction qatarienne.

En outre, l'article 50 de la loi n° (20) de 2019 portant promulgation de la loi relative à la lutte contre le blanchiment d'argent et le financement du terrorisme, prévoit également le procédé d'accès aux systèmes numériques.

II. Le régime l'infiltration numérique en droit qatarien

Contrairement au législateur français, qui a pris soin de déterminer les conditions de forme et de fond de l'infiltration numérique, le législateur qatarien n'a pas précisé le cadre juridique de l'infiltration numérique. En effet, les textes prévoyant le recours à l'infiltration numérique n'indiquent pas les conditions dans lesquelles la collecte et l'enregistrement peuvent être faites. En particulier, le législateur aurait pu préciser la durée de ce procédé et les conditions de son exécution afin de protéger les libertés individuelles, compte tenu du caractère attentatoire à la vie privée de cette mesure.

En revanche ces textes prévoient une garantie essentielle en subordonnant l'infiltration numérique à l'autorisation du ministère public, lorsqu'il estime que le recours à ce procédé est nécessaire aux fins de l'enquête.

Aussi, nous estimons que la lacune législative en ce que concerne la mise en place de l'infiltration numérique peut être complétée par l'application de l'article 77 du code qatarien de procédure pénale, qui prévoit des garanties essentielles en cas d'interception des correspondances, notamment l'exigence d'une ordonnance écrite du procureur général ou d'un juge du tribunal judiciaire, et la détermination d'un délai maximal de 30 jours renouvelable. En effet, ce texte peut constituer une soupape de sûreté en offrant un fondement juridique à l'extension des garanties qui sont prévues par l'article 77 aux procédés d'infiltration numérique qui sont prévus par la loi relative à la lutte contre la cybercriminalité et la loi de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Section 2. L'infiltration physique en matière de criminalité organisée

Définition. - Définie par l'article 706-81 du code de procédure pénale, l'infiltration consiste à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs. Cette opération est réservée aux officiers ou agents de police judiciaire spécialement habilités.

Par ces dispositions le législateur a consacré une pratique policière antérieure en matière de trafic de stupéfiants¹⁷.

Ce procédé d'infiltration se distingue d'une autre forme d'infiltration passive, appelée par le législateur la surveillance (articles 706-80 à 706-80-2).

Ainsi, après avoir étudié la notion et les conditions de l'infiltration, nous étudierons la surveillance.

Sous-section 1. Notion de l'infiltration physique

Il convient de distinguer ce procédé d'infiltration de ce que l'on appelle l'infiltration civile, avant de préciser les principes directeurs qui s'appliquent à cette mesure.

I. La distinction entre l'infiltration et l'infiltration civile

La loi du 13 juin 2025 a inséré dans le code de procédure pénale un nouveau texte, l'article 706-87-1, qui a réglementé la pratique de l'infiltration civile, laquelle consiste à autoriser un simple individu informateur à infiltrer un groupe criminel.

Cette opération qui concerne les repentis est soumise à des conditions strictes et

(17) Avant la loi de 2004, l'utilisation de la technique d'infiltration était limitée au trafic de stupéfiants.

doit être préalablement autorisée par le procureur de la République anticriminalité organisée, après avoir recueilli l'avis de la commission nationale¹⁸. La conduite de l'infiltration civile se fait sur le fondement d'une convention conclue entre le procureur de la République anticriminalité organisée et l'informateur, et elle est effectuée sous son contrôle. Cette convention doit indiquer les éléments suivants :

- La liste des délits auxquels l'informateur infiltré est autorisé à participer, qui ne peut porter sur des crimes, des délits de violences volontaires contre les personnes ou des infractions plus graves que celles dont la recherche a justifié l'autorisation de l'opération.
- La durée pour laquelle l'infiltration civile est autorisée. Cette durée ne peut pas excéder trois mois et elle est renouvelable trois fois. Elle peut être interrompue à tout moment par le Procureur de la République.
- La rétribution accordée à l'informateur infiltré ainsi que les éventuelles réductions de peine dont il bénéficie en tant que repent pour des délits commis avant la conclusion de la convention.
- Les mesures de protection et de réinsertion dont l'informateur infiltré peut bénéficier.

II. Principes directeurs

Quelques principes directeurs doivent d'emblée être rappelés, qui résultent de différents articles prévoyant l'infiltration.

a. Les autorités compétentes

La validité de ce procédé implique l'intervention de certaines personnes afin d'exécuter ou d'autoriser l'opération.

Autorités d'exécution

Seuls des officiers ou des agents de police judiciaire "spécialement habilités dans des conditions fixées par décret" peuvent réaliser ces opérations d'infiltration¹⁷.

Par ailleurs, en vue d'effectuer certaines opérations techniques, le procureur de la République ou le juge d'instruction, peut désigner toute personne physique habilitée pour la mise en place d'un système technique¹⁹.

(18) Dont la composition et les modalités de fonctionnement sont définies par décret en Conseil d'Etat 17 . Article 706-81, alinéa 2, du Code de procédure pénale

(19) Cass. crim., 23 mai 2023, n° 22-84.474 : JurisData n° 2023-008170 ; Procédures 2023, comm. 223 , J. Buisson

Autorités d'autorisation

En cas d'enquête, l'autorisation est donnée par le juge des libertés à la demande du Procureur de la République. En cas d'information, l'autorisation est donnée par le juge d'instruction, sauf pour certains actes graves réservés au juge des libertés (par exemple, la mise en place d'un système dans un lieu habité, pendant la nuit, et sans le consentement ou à l'insu de l'intéressé).

b. Les règles communes aux différents actes

Le législateur subordonne l'accomplissement des différents actes à la réunion de plusieurs conditions.

1. Il faut que la mesure soit justifiée par les nécessités de l'enquête ou de l'information d'une infraction entrant dans le champ de la criminalité organisée.
2. L'infiltration doit faire l'objet d'une ordonnance judiciaire spécialement motivée.
3. Certains actes nécessitent, à peine de nullité, l'information préalable, d'une autorité (telle l'interception de communications d'un avocat ou d'un député) ; d'autres actes sont exclus (telle la captation des données informatiques) qui ne peut être réalisés dans le véhicule, le bureau ou le domicile des avocats, parlementaires et magistrats.
4. Lorsque ces actes sont autorisés par le juge des libertés et de la détention à la requête du Procureur de la République, les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui, sont exercées par le Procureur de la République ou l'officier de police judiciaire requis par ce magistrat.

Par ailleurs les opérations sont soumises au principe de la loyauté de la preuve. Par conséquent, les opérations autorisées ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans l'ordonnance qui a autorisé l'infiltration²⁰. En revanche, le fait que ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées ne constitue pas une cause de nullité des procédures incidentes.

(20) Il s'agit là d'une application du principe de loyauté. Sur le principe de loyauté V. DANET, « Principe de loyauté et sonorisation des cellules de garde à vue », RSC 2014. 130 GALLOIS, « Loyauté des preuves pénales : la Cour de cassation est-elle allée trop loin ? » JCP 2014. 272-Crim. 7 janv. 2014, no 13-85.246 , Bull. crim. no 1 ; RSC 2014. 130, obs. Danet . – Cass., ass. plén., 6 mars 2015, no 14-84.339 , Bull. ass. plén., no 2 ; D. 2015. 711 ; AJP 2015. 362, note Girault ; RSC 2015. 117, obs. Delage.

Sous-section 2.- Conditions et effets de l'infiltration

L'opération d'infiltration est subordonnée à la réunion de certaines conditions de forme et de fond, afin qu'elle puisse produire ses effets.

I. Conditions de forme

Le législateur prévoit plusieurs règles formelles dont le non-respect est sanctionné par la nullité.

1. L'autorisation peut être accordée par le Procureur de la République ou, après avis de ce magistrat, par le juge d'instruction saisi de l'information. En outre les opérations sont exécutées sous leur contrôle respectif ²¹.
2. L'infiltration fait l'objet d'un rapport rédigé par l'officier de police judiciaire ayant coordonné l'opération, qui comprend les éléments strictement nécessaires à la constatation des infractions et ne mettant pas en danger la sécurité de l'agent infiltré et des personnes requises.
3. A peine de nullité, l'autorisation donnée est délivrée par écrit et doit être spécialement motivée.
4. Elle mentionne la ou les infractions qui justifient le recours à cette procédure et l'identité de l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération.
5. L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration.

II. Conditions de fond

Outre les conditions de forme, la validité de ce procédé implique le respect de certaines règles substantielles.

1. Le recours à l'infiltration implique préalablement l'ouverture d'une enquête ou d'une instruction portant sur l'un des crimes ou délits entrant dans le champ d'application des articles 706-73 et 706-73-1. Il s'agit des infractions graves dont la liste est déterminée par le législateur.
2. Il faut que le recours à cette mesure soit justifié par les nécessités de l'enquête ou de l'instruction.

(21) Cette exigence a un caractère constitutionnel, dans la mesure où le conseil constitutionnel, à plusieurs reprises, a posé le principe selon lequel la garantie judiciaire doit être effective, concrète et complète (Décis. 29 déc. 1983, no 83-164 DC. – Décis. 29 déc. 1984, no 84-184 DC. – Décis. 25 févr. 1992, no 92-307 DC. – Décis. 2 mars 2004, no 2004-492 DC).

3. La durée de l'opération d'infiltration doit être fixée, elle ne peut pas excéder quatre mois, et peut être renouvelée, dans les mêmes conditions de forme et de durée, ou interrompue par le magistrat l'ayant autorisée. En cas de décision d'interruption de l'opération ou à l'issue du délai fixé par la décision autorisant l'infiltration, l'agent infiltré peut poursuivre le temps strictement nécessaire pour lui permettre de cesser sa surveillance dans des conditions assurant sa sécurité sans que cette durée puisse excéder quatre mois. Informé de la poursuite de l'opération, le magistrat peut autoriser la prolongation de quatre mois afin d'assurer la sécurité de l'agent.
4. A peine de nullité, ces actes ne peuvent constituer une incitation à commettre des infractions.

Cette dernière condition constitue une simple application du principe de la loyauté²² de la preuve, qui interdit toute forme de provocation policière²³. C'est à propos de cette condition que la chambre criminelle a eu l'occasion de préciser que ne constitue pas provocation à commettre une infraction, l'acte d'achat de produit stupéfiant, réalisé par les agents infiltrés, qui s'inscrit dans le cadre des investigations antérieures à l'autorisation d'infiltration et qui mettaient déjà en évidence l'existence d'un trafic de stupéfiants, que l'infiltration ne faisait que révéler. Ainsi, l'opération d'infiltration s'est insérée dans un trafic préexistant²⁴.

Dans le même sens, la cour de cassation a considéré que ne constitue par une incitation à la commission de l'infraction, le fait pour l'agent d'infiltration qui sera chargé, en qualité de bagagiste, de récupérer les valises contenant de la drogue à l'aéroport dès lors que l'enquête démontrait que l'organisation du trafic avait débuté, de même que le fait de présenter l'agent d'infiltration comme bagagiste, alors que l'organisateur, déjà condamné pour des faits de même nature, était à la recherche d'une telle personne indispensable à l'organisation du réseau²⁵.

III. Les effets de l'infiltration

Lorsque les conditions de l'infiltration sont réunies, ce procédé entraîne des conséquences propres en autorisant à l'enquêteur l'accomplissement de certains actes incriminés. En outre, d'autres conséquences découlent nécessairement de la mise en place de ce procédé.

(22) Sur le principe de loyauté V. DANET, « Principe de loyauté et sonorisation des cellules de garde à vue », RSC 2014. 130 GALLOIS, « Loyauté des preuves pénales : la Cour de cassation est-elle allée trop loin ? » JCP 2014. 272

(23) Crim. 29 juin 2016, no 15-82.747 -Crim., 9 mai 2018, n° 17-86.558 Crim., 30 oct. 2006, n° 06-86.175 : et Crim., 30 oct. 2006, 06-86.176 Cass. crim., 9 mai 2018, n° 17-86.558.

a. Les actes autorisés

L'opération de l'infiltration, implique nécessairement l'accomplissement de plusieurs actes qui sont autorisés par les articles 706-81 et 706-82 du code de procédure pénale. Ces actes doivent être nécessaires pour la mise en œuvre ou l'exécution de l'opération d'infiltration. Ces articles listent les actes qui peuvent être accomplis.

1. Faire usage d'une identité d'emprunt. Il en résulte que l'officier de la police judiciaire et les agents adjoints peuvent utiliser de faux documents d'identité sans commettre les infractions de faux en écriture publique. Le législateur a très récemment²⁴ modifié l'article 706-81 pour ajouter une précision complémentaire à savoir que l'usage d'une identité d'emprunt peut s'accompagner de l'usage d'un dispositif permettant d'altérer ou de transformer la voix ou l'apparence physique de l'enquêteur.
2. Acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions.
3. Utiliser ou mettre à disposition des personnes se livrant à ces infractions, des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication.

b. Les effets découlant de la mise en place d'une opération d'infiltration.

Quatre effets découlent de la mise en place de l'infiltration :

1. Extension de la compétence territoriale des officiers et des agents chargés d'accomplir l'infiltration

Selon le premier alinéa de l'article 706-82 du code de procédure pénale « les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent, sur l'ensemble du territoire national » accomplir les actes autorisés par l'opération. Il en résulte que ce texte prévoit une extension aux règles de la compétence territoriale des officiers de police judiciaire qui, selon le premier alinéa de l'article 18 du code de procédure pénale, ont compétence dans les limites territoriales où ils exercent leurs fonctions habituelles²⁵.

(24) Loi n°2025-532 du 13 juin 2025 ayant modifié l'article 706-81 du code de procédure pénale

(25) Les officiers de police judiciaire ont compétence dans les limites territoriales où ils exercent leurs fonctions habituelles.

2. Admission d'un fait justificatif

En prévoyant que « les officiers ou agents de police judiciaire autorisés à procéder à une opération d'infiltration peuvent » accomplir certains actes normalement infractionnels « sans être pénalement responsables de ces actes » l'article 706-82 ne fait que rappeler le principe général posé par l'article 122-4 du code pénal, mais sans faire référence à ce texte. En effet, il résulte de ce dernier texte que l'ordre ou l'autorisation de la loi est de nature à rendre conforme à la loi un acte normalement infractionnel²⁶.

Cette autorisation de la loi bénéficie non seulement aux policiers ayant intervenus dans le cadre de l'opération d'infiltration, mais également aux autres personnes dont l'intervention était indispensable pour accomplir certains actes nécessaires à l'accomplissement de l'infiltration. Il en est ainsi des actes accomplis par des tiers à la demande des officiers ou agents qui effectuent l'infiltration.

C'est pour cette raison que le législateur a pris soin de préciser que l'exonération de responsabilité est également applicable, pour les actes commis à la seule fin de procéder à l'opération d'infiltration, aux personnes requises par les officiers ou agents de police judiciaire pour permettre la réalisation de cette opération.

3. Protection des officiers et agents ayant effectué l'infiltration

Afin de protéger les officiers et agents ayant effectué l'infiltration sous une identité d'emprunt, le législateur interdit la révélation de leur identité réelle aux différents stades de la procédure.

Cette révélation est constitutive d'un délit puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, et les peines sont aggravées lorsqu'elle a causé préjudice (des violences par exemple) aux officiers ou agents ou leur proches (art 706-84, CPP).

La loi du 13 juin 2025 a étendu cette protection aux individus qui participent à l'infiltration civile et à leurs familles²⁷.

4. Valeur de l'infiltration physique comme moyen de preuve

Cette question est régie par les articles 706-86 et 706-87 du code de procédure pénale. Ces textes affirment que peut seul être entendu en qualité de témoin

(26) Sur la notion de justification v. Magdy Habchy, « Essai sur la notion de justification », thèse, Paris Saint-Maur 1991.

(27) Loi n°2025-532 du 13 juin 2025, ayant créé l'article 706-87-1 du code de procédure pénale

sur l'opération, l'officier ayant dirigé l'opération. Mais lorsque la personne poursuivie devant la juridiction de jugement est directement mise en cause par des constatations effectuées par un agent ayant personnellement réalisé les opérations, la personne mise en cause peut demander à être confrontée avec cet agent, sans révéler sa véritable identité.

Toutefois, la question qui se pose par rapport à ce procédé est de savoir quelle valeur peut être attribuée à la preuve obtenue à la suite de l'infiltration. Cette question provient du fait que l'infiltration est fondée sur l'anonymat et par conséquent elle ne peut à elle seule fonder une condamnation en l'absence de tout élément de preuve complémentaire.

Cette solution était déjà admise par la jurisprudence de la Cour Européenne des Droits de l'Homme en ce qui concerne les témoins anonymes²⁸. La chambre criminelle, de son côté, a eu également l'occasion de montrer sa réserve par rapport à ce mode de preuve²⁹, ce qui a été confirmé par le législateur par la suite. En effet, l'article 706-87 du code de procédure pénale distingue entre deux situations selon que l'officier ou l'agent sont entendus en tant que témoin sur l'infiltration, déposent sous pseudonyme, ou selon que l'on révèle leur véritable identité. Lorsque l'officier ou l'agent déposent sous pseudonyme, dans cette situation, aucune condamnation ne peut être prononcée sur le seul fondement des déclarations faites par les officiers ou agents de police judiciaire ayant procédé à une opération d'infiltration. En revanche, lorsque l'officier ou l'agent déposent sous leur véritable identité, leur témoignage retrouve toute sa valeur en tant que moyen de preuve laissé à l'appréciation du juge et il peut fonder la condamnation.

Sous -section 3. La surveillance (l'infiltration passive)

Définition. La surveillance, qui est prévue par les articles 706-80 à 706-80-2 du code de procédure pénale, permet à l'enquêteur chargé de l'opération de demander à tout fonctionnaire ou agent public de ne pas procéder au contrôle et à l'interpellation de personnes soupçonnées, ou encore de ne pas procéder au contrôle et à la saisie d'objets, biens ou produits illicites, afin de ne pas compromettre la poursuite des

(28) CEDH 23 avr. 1997, Van Mechelen et a. c/ Pays Bas, req. no 1363/93. – CEDH 9 juin 1998, Teixeira de Castro c/ Portugal, req. no 25829/94

(29) Crim. 4 juin 1997, no 96-85.802

investigations. L'enquêteur peut également, dans le cadre de l'opération, livrer ou délivrer à la place des prestataires de services postaux et des opérateurs de fret ces objets, biens ou produits, sans être pénalement responsable.

Il en résulte que la surveillance constitue essentiellement une forme passive d'infiltration.

I. Les conditions de la surveillance

Ce procédé peut être autorisé par le Procureur de la République chargé de l'enquête ou le juge d'instruction saisi de l'information qui en avise préalablement le Procureur de la République lorsque les nécessités de l'enquête ou de l'instruction, portant sur la criminalité organisée, l'exigent. Cette autorisation, à peine de nullité, doit être écrite et motivée et versée au dossier de la procédure.

II. Les effets de la surveillance

Lorsque les conditions de la surveillance sont réunies, ce procédé entraîne deux effets.

En premier lieu, ce procédé permet l'extension de la compétence territoriale de l'enquêteur à l'ensemble du territoire national. Cette extension implique l'information préalable qui doit être donnée, par tout moyen, au Procureur de la République déjà saisi et au procureur de la République près le tribunal judiciaire dans le ressort duquel les opérations de surveillance sont susceptibles de débuter.

En second lieu, la surveillance permet l'accomplissement de deux catégories d'actes incriminés, qui deviennent justifiés par ce procédé, à savoir, d'une part, le pouvoir de l'enquêteur de demander à tout fonctionnaire ou agent public de ne pas procéder au contrôle et à l'interpellation de personnes soupçonnées, ou encore de ne pas procéder au contrôle et à la saisie d'objets, biens ou produits illicites, afin de ne pas compromettre la poursuite des investigations, d'autre part, l'enquêteur peut également dans le cadre de l'opération livrer ou délivrer à la place des prestataires de services postaux et des opérateurs de fret ces objets, biens ou produits, sans être pénalement responsable.

III. L'interdiction de la provocation policière

Le législateur a pris soin d'affirmer la règle classique de l'interdiction de la provocation policière en prévoyant dans la dernière phrase de l'article 706-80-2 que les actes autorisés ne peuvent constituer une incitation ayant déterminé la commission d'une infraction.

La cour de cassation³⁰, de son côté, a eu l'occasion de préciser le contour de cette notion en affirmant que toute méthode d'investigation qui contribuerait à provoquer la commission de l'infraction est proscrite, le stratagème ainsi employé étant alors de nature à entraîner la nullité des actes de procédure.

En revanche, et en dehors de cette hypothèse, le recours, par les autorités publiques, à un stratagème tendant à la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas, en soi, une atteinte au principe de loyauté de la preuve.

Pour qu'une telle atteinte soit constituée, il est nécessaire que le procédé employé, par un contournement ou un détournement d'une règle de procédure, ait pour objet ou pour effet de vicier la recherche de la preuve en portant atteinte à l'un des droits essentiels ou à l'une des garanties fondamentales de la personne suspectée ou poursuivie.

La loi du 15 juin 2025, a ajouté une précision complémentaire à cette notion en prévoyant que « ne constituent pas une incitation à commettre une infraction les actes qui contribuent à la poursuite d'une infraction déjà préparée ou débutée au moment où l'autorisation mentionnée au présent article a été accordée par le magistrat compétent, y compris en cas de réitération ou d'aggravation de l'infraction initiale »³¹. Cette précision textuelle est conforme à la conception jurisprudentielle de la notion de provocation policière, et au-delà, au principe de loyauté de la preuve.

Sous-section 4. L'infiltration physique et la livraison surveillée en droit qatarien

Si le législateur qatarien ne consacre aucun texte général à l'infiltration, il fait cependant référence à ce procédé dans certains textes. Nous exposons ces textes avant de préciser la nécessité d'une intervention législative afin de mettre en œuvre ce procédé en droit qatarien.

I. Les références textuelles à l'infiltration

Le législateur a prévu expressément l'infiltration dans certains textes. Il en est ainsi de l'article 50 de la loi n° (20) de 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme qui prévoit que « le ministère public peut ordonner à recourir à des méthodes d'enquête spéciales dans le cadre des instructions

(30) Assemblée plénière — 9 décembre 2019 - n° 18-86.767

(31) Le principe de loyauté de la preuve : Crim. 7 janv. 2014, no 13-85.246, Bull. crim. no 1 ; D. 2014. 407, note Vergès ; D. 2014. Pan. 1738, obs. Pradel ; AJ pénal 2014. 194, obs. Vlamynck ; RSC 2014. 130, obs. Danet ; Procédures 2014, no 83, obs. Chavent-Leclère ; Dr. pénal 2014, no 32, obs. Maron et Haas ; Dr. pénal 2014. Étude 7, obs. Bergeaud-Wetterwald

qu'il mène sur les infractions de blanchiment d'argent, les infractions initiales et les infractions de financement du terrorisme, conformément à la législation en vigueur ». Selon ce texte, ces méthodes comprennent notamment :

1. Les opérations secrètes
2. La surveillance audiovisuelle
3. L'accès aux systèmes d'information
4. L'interception des communications
5. La livraison surveillée

Toutefois, ce texte qui s'applique aux infractions de blanchiment d'argent, aux infractions initiales et aux infractions de financement du terrorisme, ne définit pas ces procédés, ni ne précise les conditions permettant d'autoriser le recours à ces procédés, ni d'ailleurs, la durée de la mesure.

Or, compte tenu du pouvoir accordé par ce texte à l'enquêteur, le législateur aurait dû subordonner la mise en place de ces procédés à l'existence des conditions de forme et de fond : l'exigence de motivation, la durée de la mesure, la détermination des actes pouvant être accomplis, et le contrôle de l'exécution de la mesure, etc.

Par ailleurs, l'article 425 du code de procédure pénale qatarien, prévoit la forme passive d'infiltration, à savoir la livraison surveillée dans le cadre de la coopération internationale.

Selon ce texte « sans préjudice des règles de compétence prévues par la loi qatarienne, le procureur général peut autoriser le passage de biens dont la possession constitue une infraction, ou qui proviennent d'une infraction ou qui ont servi à commettre une infraction, conformément aux dispositions de la législation qatarienne, à l'intérieur ou à l'extérieur du pays sans les saisir ou les remplacer totalement ou partiellement sous le contrôle des autorités compétentes, à la demande d'un État étranger, lorsque cela permet d'identifier leur destination ou d'appréhender leur auteur ». Cette disposition prévoit donc une forme d'infiltration connue en droit français sous le nom de la surveillance qui est prévue par les articles de 706-80 à 706-80-2 du code de procédure pénale.

En outre, le Qatar a signé certaines conventions internationales, notamment la Convention des Nations Unies contre la corruption du 31 octobre 2003, qui dans l'article 50³² invite les États parties à intégrer dans leurs législations, pour lutter

(32) « Afin de combattre efficacement la corruption, chaque État Partie, dans la mesure où les principes fondamentaux de son système juridique interne le permettent et conformément aux conditions prescrites par son droit interne, prend, dans la limite de ses moyens, les mesures nécessaires pour que ses autorités compétentes

contre la corruption, des mesures des livraisons surveillées et d'autres techniques d'enquête spéciales, telles que la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration. Toutefois le législateur qatarien n'a pas encore mis en œuvre ces procédés par des textes internes.

II. La nécessité d'une intervention législative destinée à la mise en œuvre de l'infiltration

Il résulte de la lecture des textes qui font référence à l'infiltration en droit qatarien deux constations.

D'une part, ces textes se contentent de faire référence aux procédés de l'infiltration directe sans en préciser la définition, ni les conditions d'application. Il en va ainsi de l'article 50 de la loi n° (20) de 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme qui prévoit, ce qu'elle appelle « les opérations secrètes et la livraison surveillée ». Ce texte est difficilement applicable dans la mesure où il ne définit pas clairement les actes entendus par ces termes. Dans ces conditions, il paraît opportun que le législateur intervienne afin de définir les termes « opérations secrètes » et « la livraison surveillée ».

En outre, et c'est la seconde constatation, cette intervention du législateur permettra de préciser les conditions de la mise en place de ce procédé ainsi que les actes qui peuvent être accomplis par les enquêteurs dans le cadre de ces opérations, à l'instar du législateur français. Cela peut être réalisée par une rédaction combinée des articles 77 du code de procédure pénale et l'article 50 de la loi sur le blanchiment, permettant ainsi au législateur de regrouper dans le code de procédure pénale l'ensemble des procédés des méthodes d'enquête spéciales, tout en précisant les conditions de recours à ces procédés.

puissent recourir de façon appropriée, sur son territoire, à des livraisons surveillées et, lorsqu'il le juge opportun, à d'autres techniques d'enquête spéciales, telles que la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration, et pour que les preuves recueillies au moyen de ces techniques soient admissibles devant ses tribunaux ».

Chapitre 2 - l'infiltration indirecte ou dissimulée

L'infiltration indirecte correspond à une infiltration dissimulée aux auteurs de l'infraction, en ce sens que la présence de la méthode d'infiltration est non seulement ignorée des auteurs de l'infraction mais, également, que l'efficacité de l'opération dépend nécessairement de cette dissimulation. Les différents procédés de l'infiltration indirecte impliquent la mise en place d'une technique ou d'un dispositif destiné à obtenir des informations portant sur l'activité criminelle supposée. Il en est ainsi des différents procédés d'accès, d'interception, ou de captation des données numériques ou informatiques.

Le législateur a récemment introduit trois nouvelles dispositions réglementant l'accès aux boîtes mails ou à la messagerie électronique en instituant, dans les articles 706-95-11 à 706-95-19 du code de procédure pénale³³, d'autres techniques spéciales d'enquête³⁴, lesquelles peuvent être mises en œuvre si les nécessités de l'enquête ou de l'information judiciaire relatives à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent³⁵. Nous exposons les règles communes aux techniques spéciales d'enquête, avant d'aborder les différentes manifestations.

Section 1. Les règles communes aux techniques spéciales d'enquête

Le législateur a pris soin de regrouper dans un paragraphe autonome les dispositions communes applicables aux autres techniques spéciales d'enquête, outre l'infiltration et la surveillance. Ces règles, qui s'appliquent en l'absence d'une disposition particulière, portent sur les conditions requises pour la mise en œuvre et l'exécution de ces techniques.

Sous-section 1. Les conditions de la mise en œuvre des techniques spéciales d'enquête

I. La nécessité d'une autorisation judiciaire

Les différents procédés des techniques spéciales d'enquête impliquent la délivrance d'une ordonnance judiciaire rendue respectivement par le juge des libertés et de la détention à la requête du Procureur de la République au cours de l'enquête et par le juge d'instruction, au cours de l'information. Cette ordonnance est rendue pour une

(33) Issu de la L. du 23 mars 2019, JO 24 mars 2019.

(34) Sous ces termes, le législateur désigne certains actes d'investigation plus ou moins intrusifs, qu'il a regroupés au sein du chapitre II, du titre XXV, du livre IV du code de procédure pénale.

(35) Cons. const., 21 mars 2019, n° 2019-778 DC

durée variable selon qu'il s'agit d'une enquête ou d'une information. Lorsqu'il s'agit d'une enquête de police judiciaire la durée maximale est d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée.

Au cours de l'information, l'ordonnance est rendue pour une durée maximale de quatre mois, renouvelable dans les mêmes conditions de forme et de durée, sans que la durée totale des opérations ne puisse excéder deux ans. Dans cette hypothèse, le juge d'instruction doit obtenir l'avis préalable du Procureur de la République, mais l'autorisation peut être délivrée sans cet avis, en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, auquel cas elle comporte alors l'énoncé des circonstances de fait établissant l'existence du risque imminent.

II. Les conditions de forme de l'ordonnance

L'article 706-95-13, rappelle quelques règles qui s'appliquent aux différents procédés d'investigation. Ainsi, l'autorisation doit faire l'objet d'une ordonnance écrite et motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires.

La jurisprudence de la chambre criminelle a considéré que cette motivation constitue une garantie essentielle³⁶ dont l'absence ferait grief aux personnes dont les propos ont été captés et enregistrés³⁷. Cependant, cette autorisation n'a pas de caractère juridictionnel et n'est pas susceptible de recours³⁸.

Sous-section 2. Les conditions de l'exécution des techniques spéciales d'enquête

Le législateur a pris soin de préciser les conditions du déroulement de ces techniques en exigeant le respect du principe de loyauté de la preuve.

I. Les conditions du déroulement des techniques spéciales d'enquête

Le législateur prévoit quatre règles pour encadrer le déroulement de ces opérations.

(36) Crim. 23 janv. 2013, no 12-85.059

(37) Crim. 6 janv. 2015, no 14-85.448 ; D. 2015. 1716, point de vue Fourment ; D. 2015. 1738, obs. Pradel

(38) Toutefois, la mesure ordonnée peut être annulée lorsque l'ordonnance n'est pas conforme aux exigences légales Sur le contrôle par la chambre criminelle de l'existence d'une ordonnance motivée fixant une durée précise v. crim. 27 févr. 2008, no 07-88.275 , Bull. crim. no 53 ; RSC 2008. 659, surobs. Buisson ; AJ pénal 2008. 284, obs. Leblois-Happe ; Dr. pénal 2008, no 76, obs. Maron et Haas ; Dr. pénal 2009. Chron. 1, p. 19, obs. Guérin ; Procédures 2008, no 156, obs. Buisson

En premier lieu, les techniques spéciales d'enquête se déroulent sous l'autorité et le contrôle du magistrat qui les a autorisées, qui peut ordonner à tout moment leur interruption.

En deuxième lieu, la mise en place de ces techniques est faite par l'officier de police judiciaire commis par le juge d'instruction ou requis par le procureur de la République ou, sous sa responsabilité, par l'agent de police judiciaire. En vue de procéder à l'installation, à l'utilisation et au retrait des dispositifs techniques, le Procureur de la République, le juge d'instruction ou l'officier de police judiciaire peut requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité ou la tutelle du ministre de l'intérieur ou du ministre de la défense et dont la liste est fixée par décret.

Un procès-verbal doit être dressé de la mise en place des dispositifs techniques et des opérations effectuées en application de la présente section. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

En troisième lieu, les enregistrements sont placés sous scellés fermés, mais l'officier de police judiciaire décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère aux infractions visées dans les ordonnances autorisant la mesure ne peut être conservée dans le dossier de la procédure.

Enfin, les enregistrements et données recueillies lors des opérations effectuées à ce titre sont détruits, à la diligence du Procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction.

II. Le respect du principe de loyauté

Enfin le législateur rappelle la règle de la loyauté de la preuve³⁹ en vertu de laquelle il est interdit tout détournement de la procédure. C'est par application de cette règle que l'article 70614-95- prévoit que « les opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat. Le fait que ces opérations révèlent des infractions autres que celles visées dans l'autorisation du magistrat ne constitue pas une cause de nullité

(39) Sur le principe de loyauté V. DANET, Principe de loyauté et sonorisation des cellules de garde à vue, RSC 2014. 130 GALLOIS, « Loyauté des preuves pénales : la Cour de cassation est-elle allée trop loin ? » JCP 2014. 272

des procédures incidentes »⁴⁰. A cette interdiction de détournement de la procédure, s'ajoute naturellement l'interdiction de la provocation policière⁴¹.

Ces règles communes s'appliquent aux différentes formes d'accès, d'interception et de captation des données numériques et informatiques, en l'absence de tout énoncé contraire.

Section 2. Les différents procédés d'infiltration indirecte

Sous-section 1. L'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique

Définition. - Ce procédé, qui est prévu par les articles 706-95 à 706-95-3, permet d'accéder à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique. Il en résulte que ce procédé peut être utilisé, non seulement en vue de l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques, mais également pour la captation des correspondances stockées.

I. Les actes autorisés

Ce procédé permet à l'officier d'accomplir certains actes, qui sont normalement incriminés, mais qui deviennent justifiés par l'autorisation de la loi.

1. L'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques, pour une durée maximale d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée.
2. L'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique. Ce procédé présente une particularité en ce sens qu'il s'applique aux crimes sans distinction et aux délits de la criminalité organisée⁴².
3. L'enregistrement, la saisie et la reproduction sur tout support des données auxquelles il a été permis d'accéder.

(40) Crim. 7 janv. 2014, no 13-85.246, Bull. crim. no 1 ; D. 2014. 407, note Vergès ; D. 2014. Pan. 1738, obs. Pradel ; AJ pénal 2014. 194, obs. Vlamynck ; RSC 2014. 130, obs. Danet ; Procédures 2014, no 83, obs. Chavent-Leclère ; Dr. pénal 2014, no 32, obs. Maron et Haas ; Dr. pénal 2014. Étude 7, obs. Bergeaud-Wetterwald

(41) Sur ce principe v. Assemblée plénière — 9 décembre 2019 - n° 18-86.767

(42) Le législateur voulait initialement étendre cette solution à l'ensemble des actes de ce cadre propre à la criminalité organisée afin qu'ils s'appliquent aux crimes même du droit commun, avant que la censure du Conseil constitutionnel n'intervienne : Cons. const. 21 mars 2019, décis. no 2019-778 DC, § 162

II. Conditions de forme et de fond

La validité de ce procédé est subordonnée à l'existence des conditions de forme et de fond.

a. Les conditions de forme

1. S'agissant de l'autorité compétente pour autoriser ces procédés, le législateur applique la même règle de répartition des compétences entre le juge des libertés et le juge d'instruction. D'une part, lorsque les faits incriminés font l'objet d'une instruction préparatoire, l'autorisation est accordée par le juge d'instruction qui instruit le dossier.

D'autre part, lorsque les faits incriminés font l'objet d'une enquête, ces procédés peuvent être accomplis sur l'autorisation, et sous le contrôle, du juge des libertés et de la détention à la requête du Procureur de la République. Le non-respect de cette exigence est sanctionné par la nullité.

Toutefois, la chambre criminelle a refusé de prononcer la nullité de la procédure d'une interception téléphonique effectuée dans une enquête préliminaire relative à un trafic de cocaïne, en raison de l'absence au dossier de la requête du procureur, dès lors que les mentions portées sur l'ordonnance du juge des libertés établissent l'existence de cette requête et en reproduisent la teneur⁴³.

Par ailleurs, la haute juridiction⁴⁴ a eu l'occasion de préciser qu'il suffit que l'autorisation soit donnée avant la mise en place de la mesure et qu'il n'est pas exigé que l'autorisation ait été transmise préalablement à l'officier de police judiciaire. Ainsi « il y a lieu de distinguer l'autorisation écrite accordée par le juge, de la transmission de ce document aux services de police ».

2. L'autorisation doit faire l'objet d'une ordonnance motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci⁴⁵.

Toutefois, lorsqu'il s'agit d'une simple interception, les dispositions de l'article 706-95 ne prévoient pas l'exigence de motivation. Or, cette absence de motivation a été invoquée comme moyen de nullité pour violation de la convention européenne des droits de l'homme, mais la cour de cassation a

(43) Crim. 5 mars 2013, no 12-88.167 ; D. 2013. 1004

(44) Crim. 26 mars 2008, no 07-88.281

(45) Crim. 8 août 2012, no 12-81.732

refusé ce moyen de défense en considérant que les dispositions de l'article 706-95 du code de procédure pénale ainsi que celles des articles 100, 100-1 et 100-3 à 100-7 auxquelles il renvoie qui ne prévoient pas que la décision du juge des libertés et de la détention autorisant des interceptions de correspondances émises par voie de télécommunications soit motivée, ne sont pas contraires aux articles 6, 8 et 13 de la Convention Européenne des Droits de l'Homme « dès lors que ces mesures, nécessaires au sens des textes conventionnels invoqués, sont autorisées par un juge qui en contrôle l'exécution et que la personne concernée dispose d'un recours effectif pour faire sanctionner d'éventuelles irrégularités qui les affecteraient » ⁴⁶.

b. Les conditions de fond

1. L'autorisation de ces procédés doit être justifiée par les nécessités de l'enquête ou de l'information.
2. La durée maximale de l'interception de correspondances est d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée. Cette durée doit être mentionnée dans le procès-verbal.

La chambre criminelle a considéré que cette exigence constitue une garantie essentielle « contre le risque d'une atteinte disproportionnée au respect du droit à la vie privée des personnes concernées, aux intérêts desquels son absence porte atteinte »⁴⁷.

Par ailleurs, la haute juridiction⁴⁸ a précisé que « la durée d'une écoute doit s'apprécier au regard de la ligne téléphonique interceptée et non de la personne qui en est titulaire, ne méconnaissent pas l'article 8 de la Convention européenne des droits de l'homme en ce que l'interception successive ou cumulée en application de ces textes de différentes lignes téléphoniques utilisées par une même personne soupçonnée d'infractions graves, est une mesure nécessaire à la défense de l'ordre et à la prévention des infractions pénales ».

3. Les interceptions sur les lignes d'un député ou sénateur, ou les lignes du cabinet ou domicile d'un avocat ou magistrat, nécessitent, à peine de nullité, l'information, selon le cas, respectivement, du président de l'assemblée, du bâtonnier, ou enfin du président ou du procureur général de la juridiction.

Par ailleurs, aucune interception ne peut porter sur une ligne dépendant du cabinet d'un avocat ou de son domicile, sauf s'il existe des raisons plausibles

(46) Crim. 27 sept. 2011, no 11-01.458, v. également Crim. 22 oct. 2013, no 13-81.945

(47) Crim. 9 janv. 2018, no 17-82.946

(48) Crim. 8 juill. 2015, no 15-81.731

de le soupçonner d'avoir participé à l'infraction qui fait l'objet de la procédure ou une infraction connexe.

Au surplus, la mesure doit être proportionnée au regard de la nature et de la gravité des faits. La décision est prise par ordonnance motivée du juge des libertés et de la détention, saisi à cette fin par ordonnance motivée du juge d'instruction, prise après avis du procureur de la République.

III. Exécution et transcription

Le législateur a pris soin d'encadrer l'exécution et la transcription de ces opérations, qui sont effectuées sous l'autorité et le contrôle du magistrat qui les a autorisées.

En premier lieu, le magistrat ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou d'un organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de communications électroniques autorisé, en vue de procéder aux opérations.

En deuxième lieu, le législateur rappelle le principe de loyauté de la preuve en interdisant le détournement de la procédure, en ce sens que ces opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision de ce magistrat.

En revanche, le fait que ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées ne constitue pas une cause de nullité des procédures incidentes.

En troisième lieu, seule la correspondance utile à la manifestation de la vérité, doit faire l'objet d'une transcription. Cette transcription est versée au dossier. Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

Afin de protéger les droits de la défense, le législateur a prévu que, sous peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense et couvertes par le secret professionnel de la défense et du conseil.

De même, à peine de nullité, ne peuvent être transcrites les correspondances avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

Sous-section 2. Du recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques

Définition. Ce procédé, qui est prévu par l'article 706-95-20 du code de procédure pénale, est destiné à fournir aux autorités de l'enquête et de l'instruction un moyen technique pour constater les infractions graves en leur permettant d'utiliser certains appareils ou dispositifs techniques, dont la mise en place ou l'utilisation est constitutive d'un délit. Il s'agit de la mise en place et l'utilisation d'un appareil ou d'un dispositif technique de nature à permettre la réalisation d'opérations pouvant constituer l'infraction des atteintes à l'intimité de la vie privée, et dont la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente est constitutive du délit puni de cinq ans d'emprisonnement et de 300 000 € d'amende par l'article 226-3 du code pénal.

Il en résulte que l'article 706-95-20 du code de procédure pénale prévoit un fait justificatif de l'infraction prévue par l'article 226-3 du code pénal.

I. Finalités et actes autorisés

Ce type de procédé peut être utilisé :

1. Afin de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé.
2. Afin d'intercepter des correspondances émises ou reçues par un équipement terminal, selon les modalités prévues aux articles 100-3 à 100-7.

Les actes autorisés et les conditions

1. Ce procédé permet d'accomplir plusieurs catégories d'actes : les actes nécessaires à la mise en place du dispositif technique. L'introduction dans un lieu privé, en vue de mettre en place ce dispositif, ou pour sa désinstallation, à l'insu ou sans le consentement du propriétaire ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur ceux-ci.
2. L'autorisation est donnée par le juge des libertés et de la détention, sur requête du procureur de la République, au cours de l'enquête, et par le juge d'instruction au cours de l'information, sauf s'il s'agit d'un lieu d'habitation et que l'opération doit intervenir pendant la nuit.

3. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge ayant ordonné la mesure.
4. La mise en place du dispositif technique ne peut concerner les lieux mentionnés aux articles 56-1, 56-2, 56-3 et 56-5 ni être mise en œuvre dans le bureau ou le domicile des personnes mentionnées à l'article 100-7. Il s'agit de certaines catégories de personnes protégées, telles les magistrats, les avocats, les locaux d'une entreprise de presse, etc.

La décision autorisant ce procédé doit comporter tous les éléments permettant d'identifier les lieux privés ou publics visés, l'infraction qui motive le recours à cette mesure ainsi que la durée de celle-ci.

II. Régime juridique

Lorsque ce procédé est utilisé pour intercepter des correspondances émises ou reçues par un équipement terminal, les règles prévues aux articles 100-3 à 100-7 s'appliquent. Celle-ci ne peuvent concerner que la personne ou la liaison visée par l'autorisation d'interception. Toutefois, à la différence des différentes formes d'interception, la durée maximale de ces procédés est de quarante-huit heures renouvelables une fois. La durée courte de ces procédés s'explique, en effet, par leur caractère instantané et leur rôle complémentaire par rapport aux autres procédés.

Néanmoins, à la différence du procédé d'interception des correspondances du droit commun (article 100 et suivants du code de procédure pénale) qui ne permet que l'interception des correspondances, le procédé qui est prévu par l'article 706-95-20 du code de procédure pénale permet également la captation des correspondances stockées.

C'est par application de cette distinction que la chambre criminelle a eu l'occasion de prononcer la nullité des captations des correspondances stockées dans le cadre d'une autorisation d'interception du droit commun. Pour la chambre criminelle⁴⁹ « N'entrent pas dans les prévisions des articles 100 à 100-5 du code de procédure pénale l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction, lesquels doivent être réalisés conformément au régime légal relatif aux perquisitions ». Cette jurisprudence condamne donc le raisonnement consistant à étendre le domaine des interceptions de correspondances émises à celles déjà stockées – et donc antérieures à l'ordonnance d'autorisation d'interception.

(49) Crim. 8 juill. 2015, no 14-88.457, Bull. crim. no 176 ; AJ pénal 2016. 90, obs. Roussel ; Procédures 2015, comm. 309, obs. Chavent-Leclère ; Dr. pénal 2015, Comm. 131, obs. Maron et Haas

III. L'articulation entre le régime de l'interception et le recueil des données

Il convient de distinguer le régime de l'interception du droit commun, qui est prévue par les articles 100 et suivants, du régime du recueil des données, qui peut également porter sur l'interception des correspondances.

Le régime de l'interception des correspondances émises par la voie des communications électroniques (droit commun). Les articles 100 à 100-8 permettent l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques, lorsqu'une information est ouverte en matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement.

Ces dispositions subordonnent ces procédés à la réunion des conditions de forme et de fond.

S'agissant des conditions de forme, la décision du juge d'instruction doit être motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci (quatre mois maximum). Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée, sans que la durée totale de l'interception puisse excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1, deux ans.

S'agissant des conditions de fond, ces procédés peuvent être ordonnés lorsque les nécessités de l'information l'exigent.

Les limites imposées par les droits de la défense. Le législateur prévoit trois règles afin de protéger les droits de la défense.

En premier lieu, l'interception ne peut porter sur une ligne dépendant du cabinet d'un avocat ou de son domicile. Toutefois, cette interception peut être ordonnée, lorsqu'il existe des raisons plausibles de le soupçonner d'avoir participé à l'infraction qui fait l'objet de la procédure ou une infraction connexe. Dans cette situation, la décision est prise par ordonnance motivée du juge des libertés et de la détention, saisi à cette fin par ordonnance motivée du juge d'instruction, prise après avis du Procureur de la République. En outre, le bâtonnier en est informé par le juge d'instruction et cette mesure doit être proportionnée au regard de la nature et de la gravité des faits.

En deuxième lieu, à peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

En troisième lieu, aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction.

Il en résulte que lorsque l'interception porte sur une ligne d'un avocat, l'interception est possible lorsque l'avocat est impliqué dans l'affaire.

C'est par application de ces règles que la chambre criminelle par un arrêt du 18 décembre 2024, a rejeté les pourvois formés par l'ancien président de la République française, Nicolas Sarkozy, son avocat, Thierry Herzog et Gilbert Azibert dans le cadre de l'affaire dite « des écoutes ».

Cette affaire est paradoxalement née d'une autre affaire, celle des conditions du financement de la campagne électorale du candidat à l'élection présidentielle de 2007 laquelle faisait l'objet d'une information ouverte, notamment des chefs de corruption, de trafic d'influence et de blanchiment. Dans le cadre de cette information, des écoutes téléphoniques ont été ordonnées sur plusieurs lignes de l'ancien chef d'État, notamment une ligne mise en service au moyen d'une carte prépayée sous le nom fictif de Paul Bismuth, mais paraissant servir à l'ancien président. Sur cette ligne, des conversations ont été interceptées entre Nicolas Sarkozy et son avocat, donnant lieu à des procès-verbaux de transcriptions, dont le contenu laissait supposer, outre le fait que les intéressés étaient informés de la mise sous écoutes des lignes régulières de l'ancien président, le fait que l'avocat recevait des informations, pour certaines confidentielles, sur un pourvoi en cassation, qui étaient en cours, devant la Cour de cassation dans une autre affaire concernant l'ancien président, dite l'affaire Bettencourt. Ces informations soumises au secret d'instruction provenaient de Gilbert Azibert, qui était alors premier avocat général près la Cour de cassation.

Ces faits de corruption active et passive ont donné lieu à une condamnation en première instance notamment des chefs de corruption et trafic d'influence, confirmée en appel. En rejetant les pourvois, en refusant la nullité d'interception des écoutes entre l'ancien président et son avocat, la chambre criminelle a rendu ces condamnations définitives. Par cet arrêt, la haute juridiction n'a fait que rappeler une jurisprudence constante⁵⁰ selon laquelle les dispositions des articles 100 et 100-7 du code de procédure pénale permettent d'intercepter des communications émises par un avocat lorsqu'il existe contre l'avocat des indices de participation à une infraction « au surplus, il ne résulte pas de la jurisprudence de la Cour européenne des droits

(50) Crim. 6 avr. 2016, n° 15-86.043, Dalloz actualité, 3 mai 2016, obs. C. Benelli-de Bénazé ; v. également, Crim. 1er oct. 2003, n° 03-82.909 P, D. 2004. 671, obs. J. Pradel ; RSC 2004. 99, obs. C. Ambroise-Castérot ; 18 janv. 2006, n° 05-86.447, D. 2006. 392, obs. C. Girault ; AJ pénal 2006. 126, obs. C. Girault ; ibid. 254, note P. Dourneau-Josette ; RSC 2006. 413, obs. J. Buisson ; 17 sept. 2008, n° 08-85.229, Dalloz actualité, 8 oct. 2008, obs. S. Lavric ; AJ pénal 2008. 467, obs. S. Lavric ; RSC 2009. 897, obs. J. Buisson

de l'homme l'interdiction d'utiliser contre le client d'un avocat les propos échangés entre eux sur une ligne téléphonique placée sous écoutes dès lors que ces propos révèlent des indices de nature à faire présumer la participation de l'avocat à une infraction pénale et qu'ils sont étrangers aux droits de la défense »⁵¹.

Sous-section 3. De l'activation à distance des appareils électroniques mobiles

Définition. Ce procédé, qui est prévu dans les articles 706-99 à 706-100 du code de procédure pénale, a pour objet l'activation à distance d'un appareil électronique mobile, à l'insu ou sans le consentement de son propriétaire ou de son possesseur, aux seules fins de procéder à la captation, la fixation, la transmission et l'enregistrement des paroles prononcées par des personnes ou de l'image de ces dernières.

I. Conditions de forme et de fond

En premier lieu, étant donné que ce procédé est de nature à porter gravement atteinte aux libertés individuelles, le législateur lui a attribué un caractère subsidiaire et exceptionnel. Ainsi, le recours à ce procédé ne peut être autorisé que lorsque les circonstances de l'enquête, ou l'instruction ne permettent pas la mise en place de la technique des sonorisations de paroles et des fixations de l'image, prévues à l'article 706-96. Ces circonstances, peuvent provenir, soit de l'impossibilité de déterminer les lieux où le dispositif technique pourrait être utilement mis en place, soit des risques d'atteinte à la vie ou à l'intégrité physique des agents chargés de la mise en œuvre de ces dispositifs.

Par ailleurs, ce procédé peut être autorisé seulement dans le cadre d'une enquête ou d'une information judiciaire relative à l'une des infractions listées par l'article 706-73, et non pas l'ensemble de la criminalité organisée.

En deuxième lieu, ce procédé peut être autorisé par le juge des libertés et de la détention, à la requête du Procureur de la République, en cas d'enquête, ou par le juge d'instruction, après avis du Procureur de la République, en cas d'information.

En troisième lieu, l'autorisation, qui est limitée à une durée strictement proportionnée à l'objectif recherché, est délivrée pour une durée de quinze jours, renouvelable une fois, en cas d'enquête, et pour une durée de deux mois, renouvelable deux fois, en cas d'information.

En quatrième lieu, la décision autorisant doit préciser l'infraction qui motive le recours à ces opérations, la durée de celles-ci ainsi que tous les éléments permettant d'identifier l'appareil. Elle est motivée par référence aux éléments de fait et de

(51) Crim., 18 décembre 2024, n° 23-83.178, §53

droit justifiant que cette opération est nécessaire et fait état des motifs attestant de l'impossibilité de recourir au dispositif technique prévu à l'article 706-96.

II. Exclusions de certaines catégories de personnes

L'article 706-100 interdit, à peine de nullité, la mise en place de ce dispositif, ou la transcription de certaines données obtenues, en ce qui concerne certaines personnes.

Ainsi, la mise en place de ce procédé ne peut concerner les appareils utilisés par un député, un sénateur, un magistrat, un avocat, un journaliste ou un médecin. Le non-respect de cette règle est sanctionné par la nullité.

Par ailleurs, à peine de nullité également, le législateur prévoit l'interdiction de transcrire certaines données relatives aux échanges avec un avocat qui relèvent de l'exercice des droits de la défense et qui sont couverts par le secret professionnel de la défense et du conseil, ou les données relatives aux échanges avec un journaliste permettant d'identifier une source, ou encore lorsque l'appareil activé se trouvait dans certains lieux, à savoir, le cabinet d'un avocat ou son domicile, les locaux d'une entreprise de presse et lieux assimilés, le cabinet d'un médecin, d'un notaire ou d'un huissier, ou, les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles.

Il appartient au juge des libertés, ayant ordonné la mise en place du dispositif, d'ordonner la destruction des données qui ne peuvent être transcrites, des procès-verbaux et des données collectées lorsque les opérations n'ont pas été réalisées conformément à son autorisation, ou lorsque les formalités prévues n'ont pas été respectées.

Sous-section 4. De la captation des données informatiques

La captation des données informatique constitue un procédé d'investigation qui peut être mis en place lorsque l'enquête ou l'instruction porte sur une infraction de la criminalité organisée.

Définition. Il s'agit de la mise en place d'un dispositif technique ayant pour objet d'accéder, sans le consentement des intéressés, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre⁵².

(52) Sur les intérêts d'investigation que présente l'utilisation de ce procédé V., Rapp. AN no 2272, XIIIe Législature, par Ciotti, p. 206 Cet acte paraît apporter une solution pertinente pour démanteler plus rapidement des groupes criminels, en donnant aux enquêteurs la faculté d'accéder à des informations dont ils ne pouvaient pas disposer jusqu'alors, ou très difficilement, car les malfaiteurs utilisent de plus en plus fréquemment des périphériques (clés USB ou CD-ROM) pour ne pas laisser dans l'ordinateur des informations susceptibles d'être découvertes lors d'une perquisition.

I. La notion de captation des données informatiques

a. Objet de la mesure

Les données, qui font l'objet de ce procédé, peuvent être stockées dans un système informatique ou elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, ou telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques (article 706-102-1 du code de procédure pénale). En vue d'effectuer ces opérations techniques, le Procureur de la République, ou le juge d'instruction peut désigner toute personne physique ou morale habilitée et inscrite sur une liste à cet effet (article 706-102-1, alinéa 3 du code de procédure pénale).

b. Distinction entre l'interception et la captation

La captation des données informatiques doit être soigneusement distinguée de l'interception

des correspondances émises par la voie de communications électroniques. Ces deux procédés se distinguent par leur nature et par conséquent ils sont soumis à deux régimes juridiques différents.

Tandis que la captation consiste à installer un dispositif⁵³ permettant d'accéder à des données déjà stockées⁵⁴ ou d'enregistrer à la source ce qu'un utilisateur saisit ou voit⁵⁵, l'interception consiste simplement à prendre connaissance en temps réel des communications électroniques au moment où elles sont émises, transmises ou reçues⁵⁶. Cette différence, explique le fait que l'interception est soumise à un régime plus souple et peut être ordonnée, en matière d'infraction du droit commun, dans les conditions des articles 100 à 100-8 du code de procédure pénale⁵⁷.

Cette distinction a été rappelée par la chambre criminelle, dans un arrêt rendu le 14 janvier 2025⁵⁸ qui a pris soin d'affirmer qu'« en l'absence de toute captation de données stockées sur des serveurs, l'interception de flux échangés par l'intermédiaire

(53) Logiciel espion, clé USB, dispositif matériel

(54) Mails, documents, images, historiques

(55) Keylogging, capture d'écran, activation micro/caméra

(56) Écoute téléphonique en direct, capture en direct des messages instantanés (WhatsApp, Signal, etc.), ou interception d'e-mails avant leur arrivée dans la boîte du destinataire, ou encore surveillance en temps réel d'un flux de données (navigation, connexions)

(57) L'interception peut être ordonnée le juge d'instruction lorsque les nécessités de l'information l'exigent, en matière de crimes, ou délits punis, au moins de 3 ans d'emprisonnement. Ces textes prévoient des conditions de fond et de forme ainsi des garanties procédurales.

(58) Crim., 14 janvier 2025, 24-84.110 24-84.116 24-85.955, Publié au bulletin

de réseaux de télécommunication ne relève pas des dispositions de l'article 706-102-1 du code de procédure pénale ». En d'autres termes, ces interceptions relèvent de l'application des articles 100 et suivants du code de procédure pénale et non pas de la procédure de la criminalité organisée.

II. Conditions de forme et de fond

Les articles 706-102-3 à 706-102-5 du code de procédure pénale prévoient plusieurs conditions de forme et de fond.

En premier lieu, ce procédé doit être ordonné par un magistrat. Le législateur applique ici le même mécanisme utilisé en matière de criminalité organisée, à savoir d'attribuer cette autorisation au juge des libertés et de la détention en cas d'enquête de police, et au juge d'instruction lorsqu'une instruction est ouverte. Toutefois lorsqu'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues au même article 59, c'est-à-dire une opération nocturne, cette autorisation est délivrée par le juge des libertés et de la détention saisie à cette fin par le Procureur de la République ou le juge d'instruction.

En second lieu, le magistrat qui autorise ce procédé doit préciser l'infraction qui motive le recours à ces opérations ainsi que la durée de ces opérations. A ce titre, l'article 706-102-3 du code de procédure pénale prévoit une nullité textuelle de la violation de cette obligation. De même, mais sous réserve de l'application de l'article 706-104, la décision autorisant ce procédé doit préciser également la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données.

Toutefois, l'article 706-104 du code de procédure pénale auquel renvoie l'article 706-102-3, prévoit la possibilité pour le juge des libertés et de la détention d'autoriser que certaines informations n'apparaissent pas dans le dossier de la procédure. Cette décision est subordonnée à l'existence de certaines conditions.

D'abord, le juge doit être saisi par requête motivée du Procureur de la République ou du juge d'instruction, cette requête doit préciser les raisons impérieuses qui justifient que ces informations ne soient pas versées au dossier de la procédure. Elle comporte toute indication permettant d'apprécier le respect des principes de proportionnalité et de subsidiarité.

Ensuite, il faut que la divulgation des informations relatives à la mise en œuvre de ce procédé soit de nature à mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches.

Enfin, cette décision peut porter seulement sur les informations relatives à la date, à l'heure et au lieu de la mise en place des dispositifs techniques, ou les informations

permettant d'identifier une personne ayant concouru à l'installation ou au retrait du dispositif technique.

Les informations non divulguées sont inscrites dans un procès-verbal qui est versé dans un dossier distinct du dossier de la procédure, il est accessible à tout moment au Procureur de la République ou au juge d'instruction et au juge des libertés et de la détention et à la chambre de l'instruction.

III. Actes autorisés et lieux protégés

Les actes autorisés. La mise en place de ce procédé permet à l'enquêteur d'accomplir certains actes incriminés sans être pénalement responsable. Ces actes sont l'introduction dans un véhicule ou un lieu privé sans le consentement de l'intéressé ou à son insu aux seules fins de la mise en place du dispositif technique ou sa désinstallation ainsi que la transmission par un réseau de communications électroniques de ce dispositif. Ces opérations ne peuvent avoir d'autre fin que la mise en place du dispositif technique ou sa désinstallation.

Il s'ensuit que le maintien en place de ce dispositif au-delà de la période autorisée, suivi de la reprise de la mesure, même autorisée par le magistrat compétent, portent nécessairement atteinte au droit au respect de la vie privée de la personne concernée par la mesure⁵⁹.

En revanche, la chambre criminelle, dans un arrêt rendu le 17 juin 2025⁶⁰, a approuvé la Chambre de l'instruction de la cour d'appel d'Aix-en-Provence ayant rejeté le moyen de nullité pris de l'envoi, par l'officier de police judiciaire au service technique national de captation judiciaire, d'une réquisition de prolongation de la mesure de captation de données informatiques avant que le juge d'instruction n'ait pris une décision d'autorisation en ce sens.

En effet, l'arrêt attaqué énonce qu'aucun grief ne saurait résulter d'une anticipation de la prolongation dès lors que celle-ci n'a pris effet que postérieurement à l'autorisation du juge d'instruction. Pour la haute juridiction, cette irrégularité, à supposer son existence, n'a pas fait grief à l'intéressé, dès lors que, en toute hypothèse, cette autorisation est intervenue avant l'expiration de la mesure initiale.

Les lieux protégés. Le législateur interdit le recours à ce procédé lorsque les systèmes automatisés de traitement des données se trouvent dans certains lieux soumis à une protection particulière.

(59) Crim., 11 juin 2024, n° 23-84.968; Procédures 2024, comm. 213, J. Buisson

(60) Crim., 17 juin 2025, 24-87.110, Publié au bulletin, V également Crim., 22 octobre 2024, 24-81.305, et Crim., 22 octobre 2024, 24-81.301, Publié au bulletin

Ainsi, est exclu de ce procédé les systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1, 56-2, 56-3 et 56-5 du code de procédure pénale. Il s'agit des lieux protégés tels que le cabinet d'un avocat ou son domicile, les locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, le cabinet d'un médecin, d'un notaire ou d'un huissier, et les locaux d'une juridiction ou le domicile d'une personne exerçant des fonctions juridictionnelles.

Cette exclusion s'explique par des considérations variées qui sont destinées à protéger les droits de la défense ou le secret professionnel, ou enfin l'immunité judiciaire.

Par ailleurs, mais dans une moindre mesure, la captation des données informatiques ne peut être réalisée, dans le véhicule, le bureau ou le domicile des avocats, parlementaires et magistrats (articles 706-102-5, alinéa 3 du code de procédure pénale).

La question des captations de données informatiques émises sur le territoire d'un Etat étranger. Lorsqu'une enquête, ou une instruction préparatoire est ouverte, une mesure de captation des données numériques peut être ordonnée. Compte tenu du principe de la territorialité, cette captation doit concerner un système automatisé de traitement des données se trouvant sur le territoire national.

En revanche, si le système se situe à l'étranger, une mesure de captation des données numériques ne peut être ordonnée sans l'intervention des autorités judiciaires de l'Etat sur le territoire duquel se trouve le système automatisé des données.

Dans le cadre européen, la directive 2014/41, prévoit deux hypothèses. Dans la première hypothèse l'intervention d'un autre Etat membre est nécessaire.

Dans cette situation prévue par l'article 30, ladite directive⁶¹ énonce qu' « une décision d'enquête européenne peut être émise en vue de l'interception de télécommunications dans l'Etat membre dont l'assistance technique est nécessaire. (...) Lors de l'émission d'une décision d'enquête européenne visée au paragraphe 1 ou au cours de l'interception, l'autorité d'émission peut également, lorsqu'elle a une raison particulière de le faire, demander une transcription, un décodage ou un déchiffrement de l'enregistrement, sous réserve de l'accord de l'autorité d'exécution ».

En revanche, lorsque l'intervention de l'autre Etat n'est pas nécessaire, dans cette situation, il incombe à l'Etat qui effectue l'interception d'informer l'autre Etat membre concerné.

(61) Intitulé « Conditions d'émission et de transmission d'une décision d'enquête européenne »,

L'article 31 de la même directive⁶² dispose que « (...) Lorsque l'autorité compétente d'un État membre qui effectue l'interception (ci-après dénommé "État membre interceptant") a autorisé, aux fins de l'exécution d'une mesure d'enquête, l'interception de télécommunications et que l'adresse de communication de la cible de l'interception précisée dans l'ordre d'interception est utilisée sur le territoire d'un autre État membre (ci-après dénommé "État membre notifié") dont l'assistance technique n'est pas nécessaire pour effectuer cette interception, l'État membre interceptant notifie l'interception à l'autorité compétente de l'État membre notifié

a. avant l'interception dans les cas où l'autorité compétente de l'État membre interceptant sait déjà, au moment d'ordonner l'interception, que la cible de l'interception se trouve ou se trouvera sur le territoire de l'État membre notifié ;

b. au cours de l'interception ou après sa réalisation, dès qu'elle s'aperçoit que la cible de l'interception se trouve ou s'est trouvée sur le territoire de l'État membre notifié au moment de l'interception »⁶³

Ces principes ont été appliqués par la Chambre criminelle dans un arrêt du 17 juin 2025. En l'espèce, la personne mise en examen invoque la nullité de la captation de données informatiques dans divers États étrangers lors du déplacement du téléphone, objet de la mesure. En rejetant cette défense, la haute juridiction a pris soin de préciser que « En effet, la captation des données informatiques, prévue à l'article 706-102-1 du code de procédure pénale qui autorise l'accès, en tous lieux, à celles-ci, s'est effectuée sans l'assistance technique des pays dans lesquels le téléphone, objet de la mesure, a été déplacé, par l'effet du dispositif technique consistant à transmettre les données vers le territoire national, le simple transit de celles-ci par le réseau d'un opérateur de l'État étranger ne caractérisant pas une atteinte à la souveraineté de cet État, de sorte qu'il n'y avait pas lieu de requérir l'autorisation de ce dernier »⁶⁴.

Sous-section 5. L'infiltration indirecte des groupes criminels en droit qatarien

Le législateur qatarien prévoit certaines manifestations de différentes formes

(62) Intitulé « Notification de l'État membre où se trouve la cible de l'interception et dont l'assistance technique n'est pas nécessaire »,

(63) V. également CJUE, 30 avril 2024, ECLI :EU:C:2024:372 la cour a considéré qu'« une mesure liée à l'infiltration d'appareils terminaux, visant à extraire des données de trafic, de localisation et de communication d'un service de communication fondé sur l'internet, constitue une « interception de télécommunications », au sens de cet article, qui doit être notifiée à l'autorité désignée à cet effet par l'État membre sur le territoire duquel se trouve la cible de l'interception. Dans l'hypothèse où l'État membre interceptant n'est pas en mesure d'identifier l'autorité compétente de l'État membre notifié, cette notification peut être adressée à toute autorité de l'État membre notifié que l'État membre interceptant juge apte à cet effet. »

(64) Crim., 17 juin 2025, 24-87.110, Publié au bulletin

d'infiltration indirecte des groupes criminels. Nous exposons ces différents procédés avant d'en préciser le cadre juridique.

I. Les différentes formes d'infiltration indirecte des groupes criminels

Le législateur qatarien a fait référence plusieurs fois aux différentes formes d'infiltration indirecte des groupes criminels.

En premier lieu, le législateur a prévu expressément dans l'article 50 de la loi n° (20) de 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme, les différents procédés de l'enquête spéciale y compris la surveillance audiovisuelle, l'accès aux systèmes d'information et l'interception des communications.

En deuxième lieu, le législateur a prévu dans l'article 77 du code de procédure pénale les différentes formes de saisis des documents postaux et les interceptions et l'enregistrement des communications.

En troisième lieu, s'agissant de l'infiltration numérique, l'article 17 de la loi n° (14) de 2014 relative à la lutte contre la cybercriminalité, prévoit que le ministère public peut ordonner la collecte et l'enregistrement immédiats de toutes les données ou informations électroniques, données de trafic ou informations de contenu qu'il juge nécessaires aux fins de l'enquête.

II. Le cadre juridique des procédés d'infiltration indirecte

Si le législateur qatarien a prévu les procédés d'infiltration indirecte, notamment dans l'article 50 de la loi relative à la lutte contre le blanchiment, il a cependant omis de préciser les conditions de la mise en œuvre de ces procédés. Cette lacune se retrouve également dans l'article 17 de la loi relative à la lutte contre la cybercriminalité, qui permet au ministère public d'ordonner les différents procédés de la collecte et de l'enregistrement des données numérique interceptées ou stockées, mais sans préciser les conditions dans lesquelles la collecte ou l'enregistrement peuvent être accomplis.

Cette lacune nécessite une intervention législative afin de poser clairement les conditions précises de la mise en œuvre de ces procédés, il est possible toutefois de trouver dans l'article 77 du code de procédure pénale qatarien une assise juridique permettant d'entourer ces différents procédés des garanties légales. Ainsi, l'article 77 peut constituer un fondement juridique de différentes formes de saisi, d'interception et de captation des correspondances et communications. Ce texte subordonne ces procédés à la réunion de trois conditions, offrant ainsi des garanties certaines pour

protéger les libertés individuelles.

En premier lieu, ce texte exige une ordonnance écrite du procureur général, lorsqu'il s'agit de certains crimes d'une particulière gravité, ou une ordonnance d'un juge du tribunal de première instance, dans les autres cas.

En deuxième lieu, ce texte exige que le procédé autorisé soit utile pour la manifestation de la vérité.

En troisième lieu, le législateur prévoit une durée maximale de la mesure de trente jours, renouvelable une ou plusieurs fois pour des périodes d'une durée équivalente, tant que les motifs justifiant cette mesure restent valables.

Il en résulte que l'article 77 du code de procédure pénale peut être étendu au-delà de son domaine actuel afin de pouvoir appliquer les garanties prévues par ce texte aux différents procédés de technique spéciale d'enquête. Cette extension peut être fondée sur le principe de l'interprétation analogique in favorem.

Conclusion

L'étude des différents procédés d'infiltration directe ou indirecte des groupes criminels, permettant de surveiller, d'infiltrer le groupe, ou permettant aux enquêteurs l'accès et la captation de données numériques émises ou stockées, mis en place par le législateur français est instructive à double titre.

D'une part, le législateur a pris soin de prévoir un système complet et cohérent, permettant de concilier la légalité procédurale et la sauvegarde des libertés individuelles en résolvant la problématique centrale qui est de concilier les exigences d'un procès équitable, le respect de la loyauté de la preuve et l'efficacité de la répression pénale. Ce régime est essentiellement structuré autour de la répartition des pouvoirs entre les différentes autorités judiciaires et policières.

Ainsi, ces techniques spéciales d'enquêtes, qui sont réservées à des policiers habilités, doivent faire l'objet d'une autorisation judiciaire préalable. Au cours de l'enquête, elles sont autorisées par le juge des libertés à la demande du Procureur de la République, et au cours de l'information ces procédés sont, en principe, autorisées, par le juge d'instruction, après avis du Procureur de la République, hormis les décisions les plus attentatoires à la liberté qui sont réservées, même dans le cadre de l'instruction, au juge de libertés, tel est le cas de l'installation d'un dispositif technique dans un lieu habité pendant la nuit.

D'autre part, le système français permet d'encadrer l'utilisation de ces procédés d'investigation afin de respecter la vie privée et les droits de la défense, à travers des garanties procédurales et exigences substantielles, dont la violation est sanctionnée par la nullité textuelle. La mise en œuvre de ce dispositif législatif a donné lieu à des jurisprudences parfois novatrices.

C'est en cherchant le point d'équilibre entre les nécessités de lutter contre la criminalité et la protection des libertés individuelles que la jurisprudence a pu trouver des solutions satisfaisantes à des questions non envisagées par le législateur.

Il en va ainsi de la question posée par l'utilisation d'un drone comme moyen d'investigation en procédure pénale. Cette question a été tranchée, en dehors de tout énoncé textuel à l'époque des faits, par un célèbre arrêt de la chambre criminelle rendu le 15 novembre 2022⁶⁵. Les faits de cette affaire sont aussi singuliers que le moyen d'investigation utilisé. En l'espèce, dans le cadre d'une instruction préparatoire ouverte contre un individu pour son implication dans un trafic de cannabis entre l'Espagne et la France, le juge d'instruction a autorisé diverses captations d'images par voie aérienne. La situation de la maison de cet individu, ayant servi de lieu de

(65) Crim., 15 novembre 2022, 22-80.097, Publié au bulletin

livraison d'une quantité importante de stupéfiants, ne se prêtant pas à une surveillance traditionnelle, le juge d'instruction a autorisé les enquêteurs, par ordonnance motivée prise après réquisitions du parquet, à procéder pour une durée de 4 mois à diverses captations d'images par voie aérienne de la maison, de son jardin et de ses abords immédiats.

En se fondant sur la généralité des termes de l'article 706-96 du code de procédure pénale, la chambre criminelle a admis la possibilité d'utiliser des caméras aéroportées comme moyen d'investigation. Ce texte prévoit qu'il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement de l'intéressé, la captation, la fixation, la transmission et l'enregistrement de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé. Ne distinguant pas selon que le dispositif technique est fixe ou mobile, ce texte englobe tout dispositif technique, ou pour reprendre la formule de la chambre criminelle « il n'y a pas à faire de distinction selon que le dispositif est fixe ou mobile, là où l'article 706-96 et les textes applicables à un tel procédé n'en font pas ».

Cette jurisprudence trouve désormais un fondement textuel dans les articles 230-47 et suivants qui a inséré dans le code de procédure pénale un nouveau chapitre VIII, au titre IV du premier livre, intitulé « les captations et fixations d'images dans les lieux publics au moyen de dispositifs aéroportés » (articles 230-47 à 230-53).

Cette extension législative et jurisprudentielle des moyens d'investigations pour englober des dispositifs aéroportés doit engendrer une mutation profonde de la politique criminelle.

Par ailleurs, le conseil constitutionnel a eu l'occasion de préciser la conformité des dispositions de l'article 706-102-1 du code de procédure pénale permettant au Procureur de la République, au cours de l'enquête, et au juge d'instruction, au stade de l'instruction, de recourir aux moyens de l'État soumis au secret de la défense nationale pour réaliser les opérations techniques nécessaires à la captation et à la mise au clair des données informatiques. Ces dispositions ont pour effet de soustraire au débat contradictoire les informations relatives à ces moyens.

S'agissant de l'étude du droit qatarien, deux conclusions peuvent être retenues. D'une part, nous avons vu que le législateur qatarien prévoit certaines manifestations de différentes formes d'infiltration des groupes criminels. D'autre part, il est apparu que le législateur a omis de préciser les conditions de la mise en place de ces procédés. Il en va ainsi de l'article 50 de la loi n° (20) de 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme qui vise « les opérations secrètes et la livraison surveillée », sans définir ces procédés, ni en préciser les conditions d'application.

Si cette lacune nécessite une intervention législative, il est cependant juridiquement possible d'étendre les garanties prévues par l'article 77 aux différents procédés d'infiltration directe ou indirecte des groupes criminels par application du principe de l'interprétation analogue in favorem.

En somme, en droit français comme en droit qatarien, l'infiltration illustre parfaitement la tension permanente entre efficacité répressive et respect des droits fondamentaux. Encadrée par un dispositif légal strict, elle permet de combattre des formes de criminalité particulièrement opaques, à condition de respecter un ensemble de garanties destinées à préserver la loyauté du procès pénal. Bien qu'elle demeure une technique dérogatoire et exceptionnelle, l'infiltration des groupes criminels s'impose aujourd'hui comme un instrument indispensable, à utiliser avec prudence et sous contrôle étroit du juge, afin d'assurer un juste équilibre entre sécurité et liberté.

Propositions

L'examen de l'infiltration des groupes criminels, en tant que mode d'investigation, nous permet de faire trois propositions.

La première proposition porte sur la tendance du législateur français qui consiste à sur-additionner les cadres juridiques, même si tous ces cadres couvrent la même opération. Le procédé d'interception et d'enregistrement des correspondances émises par la voie des communications électroniques en fournit une parfaite illustration. Il serait donc opportun, et surtout plus lisible, que le législateur regroupe dans le même article les différents procédés ayant le même objet.

Du reste, sur le plan rédactionnel, les textes faisant l'objet de notre étude peuvent être reformulés afin d'éviter les répétitions inutiles des mêmes règles. Il en est ainsi, par exemple, de la règle selon laquelle « les opérations ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du magistrat. Le fait que ces opérations révèlent des infractions autres que celles visées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes ». Ce principe, qui constitue une simple application du principe de loyauté de la preuve, peut faire l'objet d'un seul texte applicable à tout procédé de preuve.

Il en va également ainsi de la formule selon laquelle « ces techniques spéciales d'enquête peuvent être mises en œuvre si les nécessités de l'enquête ou de l'information judiciaire relatives à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent ». Ce principe, qui est prévu pour chaque procédé devrait être formulé une fois pour toutes dans un texte commun.

Il nous paraît par ailleurs nécessaire, et c'est la deuxième proposition, d'intégrer l'infiltration numérique dans un régime unifié d'infiltration, étant donné que le

système français n'est vraisemblablement pas encore optimal concernant l'infiltration dans les environnements numériques (forums, darknet).

S'agissant du droit qatarien, il nous apparaît que législateur qatarien peut s'inspirer de l'évolution du droit français, en empruntant les dispositions qui régissent l'enquête et l'instruction préparatoire, notamment l'utilisation des moyens d'investigation qui sont destinés à lutter contre l'évolution des moyens techniques nouveaux, lesquels peuvent être utilisés par les criminels, en particulier en matière de criminalité organisée et de criminalité transfrontalière.

Certes, le législateur qatarien a fait référence aux différents procédés d'enquête spéciale dans l'article 50 de la loi n° (20) de 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme, en prévoyant expressément les différents procédés de l'enquête spéciale, à savoir, les opérations secrètes, la surveillance audiovisuelle, l'accès aux systèmes d'information, l'interception des communications et la livraison surveillée, mais ce texte ne précise cependant pas les conditions de la mise en place de ces différents procédés. Cette lacune nécessite une intervention législative permettant d'étendre les garanties prévues par l'article 77 du code de procédure pénale aux différents procédés de technique spéciale d'enquête, et c'est notre troisième proposition.

Bibliographie

- M. AUDIBERT, L'extraction et l'exploitation de données contenues dans des supports numériques, AJ pénal 2023. 116
- B. AUROY, La preuve numérique en procédure pénale : un système à [re]construire, D. 2023. 697
- A. CAPRIOLI E , P. AGOSTI, La confiance dans l'économie numérique. Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique : LPA 3 juin 2005, n° 110
- B. DREVET, Les actes d'investigation non réglementés : la relative légalité procédurale, Dr. pénal 2023
- G. DUMÉNIL, La nécessité urgente d'encadrer procéduralement la mesure de cyber-infiltration, Dr. pénal 2018. Étude 22
- S. GUINCHARD et J. BUISSON, Procédure pénale : LexisNexis, 17e éd., 2024
- N. JEANNE, De l'extension de la procédure de flagrance aux infractions connexes à l'infraction flagrante et autres précisions sur les actes de l'enquête, RSC 2018. 145
- A. LEPAGE, La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet : Comm. com. électr. 2014, comm. 73
- MAYAUD, De la loi au Conseil constitutionnel, une réforme contrastée de la procédure pénale, AJP 2019. 176
- A. MORNET, Vers un droit commun de la preuve numérique ? Lexbase pénal févr. 2023, N. 43
- J. PRADEL, Procédure pénale, Cujas, 20e éd., 2019
- J. PRADEL, Notre procédure pénale à la recherche d'une efficacité à toute vapeur. Loi n° 2019-222 du 23 mars 2019, JCP 2019. Étude 406
- A. PLANTEVIN, Les propositions sexuelles faites à un mineur de quinze ans par un moyen de communication électronique, Gaz. Pal. 27 oct. 2012, n° 301, p. 24
- M. QUEMENER, Infiltrations numériques et enquêtes sous pseudonyme, JurisClasseur Communication, Fasc. 1110
- A.-G. ROBERT, Délit de propositions sexuelles faites à un mineur de quinze ans

par un moyen de communication électronique : RSC 2008, chron. p. 867

- S. SONTAG-KOENIG, Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel, AJ pénal 2016. 238
- E. VERGES, Procédure pénale, LexisNexis, 5e éd., 2017
- S. VERGNOLLE, Clair-obscur autour de la qualification des codes de déverrouillage des téléphones et des personnes pouvant les requérir, D. 2021. 609

Bibliographe en langue arabe

- Dr Ahmed Mahmoud Khalil, Manuel de procédure pénale qatari, Dar Al-Ketab Wal-Derasat Al-Arabiya, 2017
- Dr Amr Ibrahim Al-Waqad, Traité de procédure pénale qatari, Ministère de l'Intérieur, 2017
- Dr Ahmed Mahmoud Khalil, Précis de procédure pénale qatari, Dar Al-Ketab Wal-Derasat Al-Arabiya, 2017
- Dr Ghanam Mohamed Ghanam, Précis de procédure pénale qatari, Faculté de droit, 2017
- Dr Mahmoud Mohamed Sweif, L'Encyclopédie pénale : Répertoire et commentaire du code de procédure pénale qatari, Dar Al-Jami'a Al-Jadida, 2024
- Dr Mahmoud Mohamed Sweif, Le ministère public en droit qatari : commentaire des principes les plus importants de la Cour de cassation, Dar Al-Jami'a Al-Jadida, 2023
- Dr Mohamed Mahfouz, Précis du droit pénal qatari, Maison d'édition et de distribution Al-Atrash, 2018