Revista Científica del Centro Universitario de la Guardia Civil

Revista Lógos Guardia Civil

Collaboration

COOPÉRATION ENTRE LES SERVICES RÉPRESSIFS ET LES POURSUITES PÉNALES : UNE CONSTRUCTION PARALLÈLE ?

Traduction en français à l'aide de l'IA (DeepL)

Adriano J. Alfonso Rodríguez
Docteur en droit
Professeur de droit-criminologie UNED-Lugo. Juge(s)
ajalfonsorodriguez@hotmail.com
ORCID : 0009-0005-2821-4603

Reçu le 14/05/2025
Accepté le 14/05/2025
Publié le 27/06/2025

Citation recommandée : Alfonso, A. J. (2025). Coopération entre les services répressifs et les poursuites pénales : construction parallèle ? *Revista Logos Guardia Civil*, 3(2), p.p. 13-34.

Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

ORCID : 0009-0005-2821-4603

COOPÉRATION ENTRE LES SERVICES RÉPRESSIFS ET LES POURSUITES PÉNALES : UNE CONSTRUCTION PARALLÈLE ?

Résumé : PRÉFACE. 2. LE MODÈLE D'AUTORISATION JUDICIAIRE POUR LES ACTIVITÉS DE LA CNI 3. LE MODÈLE NORD-AMÉRICAIN : LA COUR FISA ET LE MUR QUI S'ÉCROULE 4. LA "CONSTRUCTION PARALLÈLE" ET LA COMMUNICATION DE RENSEIGNEMENTS ENTRE LES AGENCES 5. CONCLUSIONS 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : L'existence de deux types de sécurité, nationale et publique, a servi à habiliter différents organismes à la prévenir. Les services secrets ont acquis un rôle prépondérant dans la sécurité nationale, tandis que la sécurité publique implique la présence d'organes de police. Dans les deux cas, le travail de surveillance et de protection nécessite une violation autorisée des droits fondamentaux. Cependant, la même norme n'existe pas lorsque les services secrets sont impliqués, ce qui s'explique par le fait qu'ils n'enquêtent pas sur un acte criminel et par la communication problématique des informations obtenues, lorsqu'elles apparaissent, aux forces de police. Une stratégie de dissimulation de la source est-elle nécessaire ? En bref, une construction parallèle est-elle nécessaire ?

Resumen: La existencia de dos tipos de seguridad, la nacional y la pública, ha servido para apoderar a organismos diferentes sobre su prevención. Los servicios secretos han adquirido un protagonismo destacado en lo que respecta a la nacional, mientras que la pública implica la presencia de órganos policiales. Para el trabajo de vigilancia y protección es necesario en ambos casos vulnerar, autorizadamente, los derechos fundamentales. Sin embargo, no existe el mismo estándar cuando participan los servicios secretos que se ve rebajado por no estar investigando un hecho delictivo y la problemática comunicación de la información obtenida, cuando aquel aparece, a las fuerzas policiales ¿Es necesaria una estrategia de ocultación de la fuente? ¿Es precisa, en definitiva, una construcción paralela?

Mots clés : sécurité publique, sécurité nationale, police, service de renseignement, garanties procédurales.

Palabras clave: Seguridad pública, Seguridad nacional, Policía, Servicio de inteligencia, Garantías procesales.

ORCID : 0009-0005-2821-4603

ABBREVIATIONS

Art. 2 : Article.

CE : Constitution espagnole.

PC : Code pénal.

CESID : Centro Superior de Información de la Defensa.

CIA : Central Intelligence Agency.

CITCO : Centre de renseignement sur le terrorisme et le crime organisé.

CNI : Centre national de renseignement.

DEA : Drug Enforcement Agency (Agence de lutte contre la drogue).

DIA : Agence de renseignement de la défense.

MS : Exposé des motifs.

FBI : Federal Bureau of Investigation (Bureau fédéral d'enquête).

FJ : Base juridique.

LOPJ : Loi organique du pouvoir judiciaire.

LOPSC : Loi organique pour la protection et la sécurité des citoyens.

LSN : Loi sur la sécurité nationale.

NSA : Agence nationale de sécurité

SAN : Audiencia Nacional statuant.

SECED : Service central de documentation.

SED : Secrétaire d'Etat Directeur.

SIAM : Service d'information du personnel d'encadrement.

STC : Décision de la Cour constitutionnelle.

STS : Arrêt de la Cour suprême.

SC : Cour suprême

1) PRÉFACE.

Depuis les attentats contre les tours jumelles de New York le 11 septembre 2001 - et leurs douloureuses répliques le 11 mars 2006 à Madrid - nous sommes confrontés à un monde convulsif, où les systèmes démocratiques doivent faire face à différents fronts ouverts, allant des conflits armés à la criminalité transnationale organisée, sur fond de risques terroristes persistants ou d'espionnage mené par des pays hostiles. De manière moins conventionnelle, nous devons également être attentifs aux cyber-attaques ou aux campagnes de désinformation, réagir aux flux migratoires irréguliers, aux catastrophes climatiques et aux pandémies mondiales, ou encore à l'insécurité économique. Ces faits reflètent un monde éloigné de la paix perpétuelle et expriment une "société du risque" qui implique de faire face à une situation d'agitation, non pas provoquée par des menaces mais par les individus qui les manifestent (Beck, 2006, p. 107).

Face aux défis qui se présentent, tous très variés, avec des racines différentes et des solutions complexes, nous nous trouvons dans la sphère de ce que l'on appelle la protection de la "sécurité nationale", un concept qui a été expliqué sous différentes perspectives. Cependant, dans notre pays, la réglementation de ce concept est très récente, à peine dix ans, et vise à fournir un cadre réglementaire à un espace qui, traditionnellement, était placé dans l'ombre parce que l'on considérait que l'action de l'État dans certains domaines devait rester strictement secrète, en contraste évident avec l'idée de "sécurité publique", dont la présence législative est beaucoup plus ancienne, obligatoire en démocratie, et basée sur l'idée que gouverner implique le pouvoir de contenir le pouvoir de police (Zaffaroni, 2006, p. 165).

En tout cas, notre texte constitutionnel (ci-après CE) n'a pas abordé l'idée de "Sécurité Nationale", ni envisagé une définition en tant que telle, bien qu'il fasse allusion au concept de "Sécurité Publique" dans divers préceptes de notre lex supérieure en établissant la garantie de la "sécurité des citoyens" par les forces de police (art. 104.1 CE) ou la propriété exclusive de l'Etat de la "sécurité publique" (art. 149.1.29ª CE).L'art. 149.1.29ª CE) ou la propriété exclusive de l'État sur la "sécurité publique" (art. 149.1.29ª CE), sans oublier l'art. 126 CE qui parle d'une "police judiciaire" dans une situation de dépendance des juges et des procureurs dans l'enquête sur le crime et la découverte de l'auteur du délit (*Cfr.* SSTC 175/1999, du 30 septembre, FJ 7º 86/2014, du 29 mai, FJ 4º ou 55/1990, du 28 mars, FJ 5º). Cette situation, non reconnue, n'a pas empêché l'idée de "Sécurité nationale" d'émerger comme un outil singulier de protection, comme une politique à part entière, bien que sans ministère pour la gérer (Herbon Costas, 2021, p. 164). Cependant, cela ne nous empêche pas de constater que les deux "sécurités" opèrent dans les mêmes sphères, touchent des aspects similaires et se fixent des objectifs identiques, et bien que les droits fondamentaux puissent être violés à ces deux niveaux, elles opèrent selon des critères différents, plus souples dans leur dimension éthique lorsqu'il s'agit de sécurité nationale, et qui laissent en suspens l'existence d'un pont à franchir en cas de collaboration entre les différentes instances opérationnelles chargées de veiller à leur accomplissement.

D'un point de vue réglementaire, l'article 3 de la loi 36/2015 du 28 septembre sur la sécurité nationale (ci-après LSN) stipule que "Aux fins de cette loi, on entend par sécurité nationale l'action de l'État *visant à protéger la liberté, les droits et le bien-être des citoyens, à garantir la défense de l'Espagne et de ses principes et valeurs constitutionnels,* ainsi qu'à contribuer, avec nos partenaires et alliés, à la sécurité internationale dans le respect

des engagements pris". Conformément à cette définition, l'idée de "sécurité publique" dans l'exposé des motifs (EM) de la loi organique 4/2015, du 30 mars, sur la protection de la sécurité publique (LOPSC) stipule que "la loi, conformément à la jurisprudence constitutionnelle, se fonde sur un concept matériel de sécurité publique compris comme une activité *visant à protéger les personnes et les biens et à maintenir la tranquillité des citoyens*, qui englobe un ensemble pluriel et diversifié d'actions, différentes par leur nature et leur contenu, visant le même objectif de protection du bien juridique ainsi défini. Dans cet ensemble d'actions s'inscrivent les actions spécifiques des organisations instrumentales destinées à cette fin, notamment celles correspondant aux Forces et Corps de Sécurité, auxquels l'article 104 de la Constitution *confie la protection du libre exercice des droits et des libertés et la garantie de la sécurité publique...*".

Il est facilement perceptible, comme cela a été souligné, l'idée commune de la protection des libertés et des droits qui place les deux concepts dans un fil conducteur clair, que nous pouvons même observer dans la jurisprudence. En ce sens, le STC 184/2016, du 3 novembre, le premier arrêt qui a abordé le concept de "sécurité nationale", affirme "*D'autre part, étant donné que la compétence de l'État est claire, tant en matière de défense que de sécurité publique, il ne serait pas logique que, dans un domaine tel que la sécurité nationale, si étroitement lié aux deux, au point d'identifier ses buts et objectifs et les biens juridiques protégés de la manière indiquée, la compétence de l'État devienne purement résiduelle". En définitive, la sécurité nationale n'est pas une nouvelle compétence**, mais elle est intégrée** dans les compétences étatiques de défense et de sécurité publique*" (FJ 3º). Cet arrêt, qui ne fait que lier les deux concepts, n'empêche pas d'établir des différences claires.

Tout d'abord, la défense de la sécurité nationale contre les menaces, par l'obtention d'informations, est du ressort des services secrets, notamment, dans notre pays, du Centre national de renseignement (CNI). En ce qui concerne la sécurité publique, ou sécurité des citoyens, sa protection est confiée aux services de police, qu'il s'agisse de l'administration centrale, régionale ou locale. D'autre part, les services secrets, dans le cadre de la surveillance des activités susceptibles d'affecter la sécurité nationale (espionnage, contre-espionnage, lutte contre le terrorisme, etc.), opèrent selon un critère clair d'extrême discrétion opérationnelle, de sorte que leur travail reste sous le couvert d'informations classifiées, qui ne sont pas connues du public, et que les résultats de leur travail sont rarement portés devant un tribunal, situations qui n'affectent pas le travail des forces de sécurité, qui exercent leurs activités sous le contrôle d'organes judiciaires, avec des résultats qui sont publics et rendus publics, l'objectif ultime étant de conduire, en règle générale, à la détermination, ou non, de la responsabilité pénale à élucider par les tribunaux. Quatrièmement, la violation organisée des droits fondamentaux requiert, tant dans le travail de la police que dans celui du CNI, une autorisation judiciaire, alors que le cadre procédural pénal dérivé de la loi de procédure pénale (LECRIM) agit comme une bride pour les agences de sécurité publique, les services secrets opèrent dans un cadre nécessairement plus large où la réglementation normative est plutôt limitée, à travers le seul article contenu dans la loi 2/2002, du 6 mai, avec un contrôle judiciaire limité à l'autorisation de mesures affectant le secret des communications et les perquisitions à domicile qui affectent partiellement l'article 18 CE, l'objectif étant de collecter des informations sur les activités des services secrets. 18 CE, son but étant la collecte d'informations dont la destination n'est pas, en principe, un procès. Cependant, plusieurs questions se posent : quel est notre modèle de contrôle judiciaire des activités de renseignement ? Est-il possible pour les services secrets de partager des informations avec

les services de police ? Serait-il possible de les utiliser dans le cadre d'enquêtes et de poursuites pénales ? Examinons différents aspects permettant de formaliser le débat.

2. LE MODÈLE D'AUTORISATION JUDICIAIRE POUR LES ACTIVITÉS DES CNI.

La collecte traditionnelle de renseignements par les services d'espionnage a toujours été basée sur des techniques clandestines, avec une dimension éthique nécessairement flexible dans son développement et un cadre assez flou de garanties pour les personnes concernées. Plus la menace est grande, plus les méthodes d'obtention d'informations sont complexes, où l'évaluation et l'analyse deviennent des outils de précision pour déterminer la réponse, l'action ou la décision. En fait, l'importance des services secrets dans une démocratie réside dans le fait qu'ils aident l'exécutif à suivre des lignes spécifiques pour défendre les intérêts nationaux, devenant ainsi des acteurs importants dans la prise de décision politique (Pinto Cebrián, 2019, pp. 51 et suivantes). Ils n'ont rien à voir avec l'enquête sur l'acte criminel, ni avec l'auteur de l'infraction ou leur poursuite procédurale (Sánchez Ferro, 2020, p. 188-189), sans oublier que c'est précisément la sécurité nationale qui justifie leurs fonctions et permet la violation, bien qu'ordonnée, des droits fondamentaux (Aba Catoira, 2020, p. 228).

Dans notre pays, comme je l'avais prévu, le CNI, organe de l'administration générale de l'État de nature unique (SAN 2632/2009, 27 mai, Sala de lo Contencioso (Rapporteur : M. Gil Ibáñez, FJ 1º), dépendant de l'exécutif et qui *"... n'est pas, ni n'est assimilé à* un organe identifié à une administration indépendante, au sens de cette typologie d'entités de droit public dotées de l'autonomie et de l'indépendance fonctionnelle qui les caractérisent : c'est un organe instrumental du gouvernement...*".n'est pas, ni ne peut être assimilé à un organisme identifié à une administration indépendante, au sens où ce type d'entité de droit public est doté de l'autonomie et de l'indépendance fonctionnelle qui le caractérise : c'est un organe instrumental du gouvernement...*" (STS 1238/2021, du 18 octobre, Chambre III, (Rapporteur : M. Requero Ibáñez) FJ 7º) , ce qui reflète, dans sa physionomie, une longue évolution dans l'histoire de nos services. Ainsi, il a succédé au Centre supérieur d'information de la défense (CESID), lui-même créé par le décret royal 1558/1977 du 4 juillet 1977, organisme qui regroupait les services d'information précédents, le Service central d'information de la présidence du gouvernement (CESED) et le Service d'information du haut état-major général (SIAM), Il a toujours agi en tant qu'organe d'évaluation des renseignements et, au cours des différents gouvernements, il a dépendu du ministère de la Défense, à l'exception d'une période de dépendance vis-à-vis du ministère de la Présidence pendant le gouvernement de Mariano Rajoy Brey. Son intégration initiale avec les membres des forces armées a fini par évoluer avec l'incorporation de personnel civil, de sorte que cet organisme ne peut plus être considéré comme un simple compilateur de renseignements militaires face à un éventuel conflit militaire. Son travail va au-delà, car les menaces sont de plus en plus hétérogènes, avec des conflits asymétriques qui se développent sur des champs de bataille invisibles et dont l'existence et l'intervention sont essentielles pour y faire face.

Conformément à l'article 9 de la loi 11/2002 du 6 mai 2002, le CNI est dirigé par un secrétaire d'État **(**SED), qui est l'"autorité nationale de renseignement et de contre-espionnage" avec le titre de "directeur", nommé par décret royal sur proposition du ministère de la défense, et avec un mandat de cinq ans qui peut être successivement prolongé ou remplacé à tout moment par le gouvernement. Ses fonctions sont de

"promotion" et de "coordination", ce qui peut se résumer par la "direction" des tâches de l'organisme, la nomination des différents postes de direction, la compétence budgétaire et la coopération "*avec les services d'information des Forces et Corps de Sécurité de l'État*, et les organes de l'Administration civile et militaire, en rapport avec les objectifs d'intelligence...". Il est assisté d'un secrétaire général, ayant rang de sous-secrétaire, qui, entre autres fonctions, en plus de le remplacer, est chargé de "diriger le fonctionnement des services communs du Centre par le biais des instructions et des ordres de service correspondants" (art. 10, loi 11/2002). Il s'agit donc des principaux responsables des fonctions de responsabilité du CNI, avec l'existence possible et hypothétique de la Division du renseignement extérieur, de la Division du contre-espionnage, de la Division du renseignement intérieur, de la Division de l'économie et de la technologie, ainsi que de la Sous-direction générale de l'administration et des services et de la Sous-direction générale du personnel et d'un Bureau de conseil juridique, d'un Bureau technique, d'un Chef du soutien opérationnel et d'un Service de sécurité (art. 1 et 2 du RD 2632/1985). 1 et 2 RD 2632/1985, du 27 décembre 1985, bien que plus tard, dans le RD 266/1996, du 16 février 1996, l'art. 2 établisse l'existence d'unités d'intelligence et d'unités d'appui opérationnel et technique avec une unité de sécurité chargée des tâches de protection). En tout état de cause, il est possible que cette organisation interne soit très différente aujourd'hui.

Parmi toutes les questions, il y en a une qui revêt une grande importance face à une histoire qui a placé le travail de nos services secrets dans l'ombre. Il s'agit des activités de renseignement dans le cadre desquelles des perquisitions et des écoutes téléphoniques ont été réalisées, un scénario orphelin de toute réglementation et extrêmement problématique jusqu'à la loi 2/2002, du 6 mai, qui, en un seul précepte, avec un impact par le biais de sa loi transitoire sur la loi organique du pouvoir judiciaire 6/1985, du 1er juillet, (LOPJ), dans les articles 125, 127, 135, ainsi que le nouvel article 342 bis de la même loi, a permis d'améliorer les conditions de travail des services secrets. 125, 127, 135, ainsi que le nouvel art. 342 bis du même texte, décide que c'est un juge du Tribunal suprême (deuxième chambre pénale ou troisième chambre administrative) qui sera chargé d'autoriser le CNI à effectuer des actes touchant à l'inviolabilité du domicile (art. 18.2 CE) et à l'interception des communications (art. 18.3 CE). Il s'agit d'un système inhabituel (Lanz Muniain, 2023, p.27), sans équivalent dans nos pays voisins, à l'exception, avec des nuances relatives, des Etats-Unis, comme nous le verrons, l'attribution de la compétence à un juge unique, et pour une période temporaire de cinq ans, n'est pas exempte de critiques pour s'éloigner du sens constitutionnel du juge ordinaire prédéterminé par la loi (De la Oliva Santos, 2006, p. 154). Il est clair qu'un tribunal d'espionnage n'a pas été correctement créé.

La justification de l'amendement est fournie par l'EM de la loi 2/2002 qui stipule que "pour les activités susceptibles d'affecter l'*inviolabilité du domicile et le secret des communications*, la Constitution espagnole exige, dans son article 18, une autorisation judiciaire, et l'art. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales exige que cette ingérence soit prévue par la loi et constitue une mesure qui, dans une société démocratique, *est nécessaire à la sécurité nationale, à la sûreté publique*, au bien-être économique du pays, à la défense de l'ordre et à la *prévention des infractions pénales*, à la protection de la santé ou de la morale, ou à la *protection des droits et libertés d'autrui*". Comme on peut le voir, il fait allusion aux deux garanties et aux aspects qui les nourrissent en tant qu'élément justifiant la violation de l'article 18 CE et sur la toile de fond de la protection des droits et des libertés, un élément central des

deux garanties.

Le modèle d'autorisation est extrêmement particulier, réglementé dans l'article unique de la loi 2/2002, du 6 mai, et en synthèse est initié par le SED, qui soumet au magistrat SC (Chambre II ou III), élu par le Conseil général du pouvoir judiciaire (CGPJ) pour une période de cinq ans - coïncidant avec le mandat du SED - une requête pour violation des droits fondamentaux, qui doit être dûment motivée et contenir nécessairement les points suivants : " *a) Spécification des mesures demandées. b) Les faits sur lesquels la demande est fondée, les objectifs qui motivent la demande et les raisons qui conseillent l'adoption des mesures demandées. c) L'identification de la personne ou des personnes affectées par les mesures, si elle est connue, et la désignation du lieu où les mesures doivent être prises. d) La durée des mesures demandées, qui ne peut excéder vingt-quatre heures dans le cas de l'inviolabilité du domicile et trois mois pour l'intervention ou l'interception de communications postales, télégraphiques, téléphoniques ou de tout autre type, les deux périodes pouvant être prolongées pour des périodes successives égales en cas de nécessité.* Une fois la requête déposée par le SED reçue, le juge de la CS dispose de 72 heures (ou 24 heures en fonction de l'urgence de la mesure) pour sauvegarder sa procédure, qui sera secrète. La décision judiciaire initiale, éventuellement une ordonnance, et les décisions ultérieures qui la prolongent, ne peuvent pas faire l'objet d'un appel, ni d'une révision, car les seuls acteurs de cette procédure sont le juge de la Cour suprême et la SED, qui, par ailleurs, "ordonne la destruction immédiate du matériel relatif à toutes les informations qui, obtenues au moyen de l'autorisation prévue dans le présent article, ne sont pas liées à l'objet ou à la finalité de l'autorisation".

Il est clair qu'il n'y a pas de principes qui inspirent la demande, de critères pour l'accorder ou la refuser, d'utilisation ou de destination du matériel obtenu, de contrôle judiciaire de l'exécution des mesures ou du résultat obtenu, à l'exception de la prolongation, de la situation des personnes affectées par la mesure d'immission ou des recours contre la décision rendue. En ce sens, la justification est, a priori, que le matériel obtenu n'est pas susceptible de générer des preuves ni d'être utilisé dans une procédure pénale (González Cussac, 2015, p.88). Cependant, on ne peut pas exclure, comme premier élément de nuance, la transcendance procédurale du travail de renseignement, comme le montre l'utilisation, dans la juridiction contentieuse, des rapports de la CNI pour refuser la nationalité à des requérants étrangers pour des raisons de " sécurité nationale " (SSTS 233/2022, 23 février, Chambre III, Orateur : M. Menéndez Pérez, FJ 4º ; 395/2022, 29 mars, de la Chambre III, Rapporteur : M. Román García FJ 6º ; 367/2021, du 17 mars, de la Chambre III, Rapporteur : M. Herrero Pina FJ 2º, ; 4376/2015, du 26 octobre, de la Chambre III, Rapporteur : M. Del Riego Valledor, FJ 4º ; STS 2105/2014, du 26 mai, de la Chambre III, Rapporteur : M. Del Riego Valledor, FJ 5º). Toutefois, je reviendrai plus tard sur son utilisation dans les procédures pénales pour clarifier la question. En tout état de cause, l'objectif a été de combiner des aspects relativement antithétiques, tels que la surveillance de quelque chose qui, par nature, ne pouvait pas être surveillé, en ouvrant une voie judiciaire qui, d'autre part, ne contraint pas opérationnellement les agents en les maintenant en dehors des exigences dérivées de l'existence d'une procédure pénale ouverte (Alfonso Rodríguez, 2024, p. 132).

Le point de départ de la demande tourne autour de l'article 4 b) de la loi 11/2002, du 6 mai, qui établit, entre autres, comme principale fonction de notre service

d'espionnage celle de "*Prévenir, détecter et permettre la neutralisation des activités de services étrangers, de groupes ou d'individus qui mettent en danger, menacent l'ordre constitutionnel, les droits et libertés des citoyens espagnols, la souveraineté, l'intégrité et la sécurité de l'État, la stabilité de ses institutions, les intérêts économiques nationaux et le bien-être de la population*". En ce sens, cela reflète l'élément justificatif de la demande d'autorisation judiciaire dans l'article unique, convertissant le juge de la Cour suprême chargé de l'autorisation en interprète de concepts non juridiques tels que la "souveraineté" ou l'"intégrité", les "intérêts économiques nationaux" ou le "bien-être de la population", qui sont les objectifs ultimes du développement des tâches d'espionnage et qui, avec le respect des droits, des libertés ou de la stabilité institutionnelle, impliquent de faire de lui le gardien de la "sécurité nationale" qui permet au service d'être en mesure d'exercer ses fonctions.

La question soulevée par l'habilitation judiciaire du CNI à intercepter un téléphone ou à pénétrer dans un domicile est qu'elle implique une sorte de sauvegarde mais s'éloigne d'une fonction de garantie des droits fondamentaux (Pascual Sarria, 2007, p. 197) que, d'autre part, le pouvoir judiciaire se voit attribuer en vertu de l'art. 117.4 CE, et transforme la procédure en *une sorte de dossier secret pour demander des mesures limitant des droits fondamentaux spécifiques, dans le cadre d'opérations de renseignement pour la protection de la sécurité nationale, à un juge de la CS, soumis à un mandat temporaire et expressément désigné à cette fin* (Alfonso Rodríguez, 2023, p.89).

3. LE MODELE AMERICAIN : LA COUR FISA ET UN MUR QUI S'EFFONDRE.

Il n'est pas certain que les États-Unis aient servi de modèle pour la configuration et la physionomie de notre système de contrôle des activités de renseignement. Cependant, il est clair que nous ne pouvons pas accepter une inspiration totale, car le système procédural est éloigné entre les deux pays, avec le système accusatoire de l'Amérique du Nord dans lequel les parties (accusateur et accusé) sont les véritables "propriétaires" du processus pénal américain, et où le principe du "Due Process of Law", le droit à une procédure régulière avec toutes les garanties, se révèle être le "moteur" de l'organisation procédurale (Gómez Colomer, 2006, pp. 50-57), contrairement à un modèle de juge d'instruction béni par un juge de première instance qui est le "propriétaire" du système (Gómez Colomer, 2006, pp. 50-57), contrairement à un modèle de juge d'instruction qui est le "propriétaire" du système. 50-57), contrairement à un modèle de juge d'instruction béni par une LECRIM de 1882, ce qui est impossible, en tout état de cause, aux Etats-Unis. Cependant, il faut noter que le modèle procédural de la FISA Court ne répond pas à ce système accusatoire.

Le modèle de renseignement américain repose sur une pluralité d'agences (CIA, NSA, DIA, FBI dans sa branche renseignement, forces armées et ministères avec leurs propres services) qui sont désormais coordonnées par un directeur national du renseignement, conformément à la loi de 2004 sur la réforme du renseignement et la prévention du terrorisme (IRPA), en tant que commissaire de l'exécutif pour la coordination adéquate de toutes les organisations, coexistant avec un contrôle intense du corps législatif par le biais de commissions de contrôle parlementaires. Dans ces conditions, il est nécessaire de partir d'une phase d'abus systématiques de la part du FBI ou de la CIA, mis en évidence par la commission *Church* du Sénat (Arrieta, 2025, p. 122). Cette phase, qui s'est déroulée dans le cadre de la *loi sur la surveillance du renseignement*

étranger (*Foreign Intelligence Surveillance Act* - FISA), a conduit à la promulgation en 1978 de la *loi sur la surveillance du renseignement étranger* (*Foreign Intelligence Surveillance Act* - FISA), qui prévoyait notamment la création d'une Cour fédérale chargée de contrôler la surveillance électronique des agents étrangers aux États-Unis, composée aujourd'hui de onze juges fédéraux à l'identité publique, mais dont le travail est effectué en secret, et qui sont nommés *par le président de la* Cour suprême fédérale des États-Unis. Ce sont ces juges qui sont chargés de vérifier les demandes de l'exécutif, qui doit prouver comme "cause probable" - un soupçon raisonnable qui motive la demande - que la cible de l'écoute ou de la surveillance des dispositifs électroniques est une puissance étrangère ou un agent d'une puissance étrangère qui est la cible de l'opération de collecte de renseignements, donc que son utilisation n'était pas, a priori, destinée à intercepter les communications des citoyens américains. En l'absence d'un cas prima facie d'acte criminel pour obtenir le mandat de la Cour FISA, la norme d'autorisation est moins stricte que la norme habituelle requise par les forces de l'ordre pour violer les droits du quatrième amendement - la vie privée (Ruger, 2007, p. 243).

La demande est présentée devant un juge de la FISA Court dans laquelle le gouvernement comparaît avec sa représentation en tant qu'unique partie procédurale intervenante, où, outre la preuve de la cause probable, l'identité des personnes impliquées et des fonctionnaires impliqués, la durée des mesures de surveillance électronique, les certificats des autorités de renseignement et les détails des demandes précédentes, entre autres éléments, doivent être indiqués. Le fait que ce soit le pouvoir exécutif qui agisse en tant qu'unique participant éloigne la procédure du système accusatoire typique du système américain (Sobel, 2023, p. 15), estimant que l'une des raisons, parmi d'autres avancées à l'époque par l'*Attorney General* Griffin Bell lors de la rédaction de la loi, qui pourrait motiver l'absence d'autres participants, est due à la réticence du gouvernement lui-même à déclassifier des informations par crainte de fuites (Chin, 2021, p.665).

Au vu des données fournies, le juge de la FISA accorde ou refuse en détail le *mandat de* surveillance électronique demandé par le gouvernement, en identifiant les sujets, les moyens, le type d'informations à obtenir et la durée du mandat. Son refus peut être réexaminé devant la *FISA Court Review*, composée de trois juges du même organe, avec la possibilité de faire appel auprès de la *Cour suprême des États-Unis* si le réexamen n'aboutit pas.

Cependant, alors que jusqu'en 2001, le mandat de la FISA servait à la collecte de renseignements, les attaques terroristes du 11 septembre 2001 aux États-Unis, avec le *Patriot Act* de 2001, en vertu de l'article 203, ont modifié l'architecture de la loi et ont ainsi brisé le *mur* entre la collecte de renseignements étrangers et les enquêtes criminelles (Donohue, 2021, p. 204), permettant l'utilisation du partage d'informations par les services répressifs (FBI ou DEA), obtenues aux fins de la collecte de renseignements étrangers en vertu de la FISA, et dans les enquêtes criminelles, mélangeant ainsi une méthode identique à des fins différentes, ce qui incite les services répressifs (FBI ou DEA) à utiliser le partage d'informations pour la collecte de renseignements étrangers en vertu de la FISA, et pour les enquêtes criminelles, ce qui incite les services répressifs à utiliser le partage d'informations pour la collecte de renseignements étrangers en vertu de la FISA, et dans les enquêtes criminelles, mélangeant ainsi une méthode identique à des fins différentes. 204), autorisant l'utilisation de l'échange d'informations par les services répressifs (FBI ou DEA), obtenues aux fins de la collecte de renseignements étrangers dans le cadre de la FISA, et dans le cadre d'enquêtes criminelles, mélangeant ainsi une

méthode identique avec des objectifs différents, ce qui suscite plusieurs réflexions.

Premièrement, en vertu des normes de la demande, dans la mesure où l'accréditation de la cause probable est différente, puisque dans une enquête criminelle il était nécessaire de prouver, grâce à ce concept, la commission possible d'un acte criminel, ce qui n'est pas le cas dans la demande de mandat en vertu de la réglementation FISA. Deuxièmement, l'objectif commun étant de prévenir une attaque terroriste, la coopération et la transmission de renseignements entre les agences d'espionnage et les services répressifs, dont les tâches sont différentes, se sont accrues, et les frontières entre la communauté du renseignement et les services de police se sont donc brouillées et estompées (Stein, Mondale, Fisher, 2016, p. 2266). Troisièmement, la possibilité de monter un dossier pénal à partir d'informations obtenues selon les critères de la FISA est devenue une possibilité distincte (pensez à une affaire fédérale de terrorisme ou de narcoterrorisme dans laquelle les services répressifs ont reçu des informations d'agences de renseignement à la suite des résultats obtenus dans le cadre d'un mandat FISA), de sorte qu'un débat clair s'est instauré concernant les droits des personnes concernées à une procédure régulière et leur droit de se défendre contre le partage de matériel de renseignement entre agences (Reid, 2015, p. 429).

4. LA "CONSTRUCTION PARALLÈLE" ET LA COMMUNICATION INTER-AGENCES EN MATIÈRE DE RENSEIGNEMENT.

Suite à ce qui a été observé précédemment concernant la chute du mur, il est évident que la "sécurité nationale", un concept trop ambigu, a été intégrée à la "sécurité publique", sachant que les exigences procédurales pour la violation des droits fondamentaux, en particulier la confidentialité des communications, ont été abaissées face à la revendication de la collecte de renseignements, des renseignements qui, par la suite, à la suite d'un changement de réalité qui a entraîné une mutation des principes, ont été utilisés à des fins différentes, à la limite des coutumes procédurales et des droits fondamentaux dans des exercices d'interchangeabilité, soit pour la prise de décisions politiques, soit pour constituer la base d'un dossier pénal. C'est dans ce scénario que prend tout son sens le concept de *"construction parallèle"*, qui a commencé par la réception d'informations de renseignement avec des normes d'obtention assouplies, dont l'origine ne peut être révélée et qui, comme je l'ai souligné précédemment, pourrait bien mettre en péril les garanties procédurales en fournissant un raccourci opérationnel qui pourrait contourner les objections juridiques et qui oblige à inventer un canal parallèle qui détourne l'attention de la source originale (par exemple, un informateur créé artificiellement). Par exemple, un informateur créé artificiellement qui dissimule des informations de renseignement obtenues dans le cadre d'un mandat différent, tel qu'un mandat de la Cour FISA).

Si nous avons analysé précédemment le modèle d'obtention d'informations par le CNI, l'organe principal de notre Communauté d'Intelligence, la situation à laquelle est confrontée une agence policière, qu'il s'agisse d'une agence étatique comme la Police Nationale, la Garde Civile ou le Service de Surveillance Douanière ou les cas de Polices Autonomes expressives d'un modèle intégral (STC 184/2016, du 3 novembre, FJ 4º) comme la Catalogne, la Navarre et le Pays basque, qui disposent chacune d'unités d'information et qui constituent une sorte de " Communauté d'intelligence policière " où le Centre d'intelligence sur le terrorisme et le crime organisé (CITCO) intervient en tant qu'organe d'analyse et de coordination entre les organismes. Toutefois, il convient de souligner que, dans le cadre de la collecte de renseignements, les forces de police sont

soumises à des contraintes procédurales, dans le cadre de la satisfaction de la sécurité publique, qui sont radicalement différentes de celles des services de renseignement, et où l'autorité judiciaire agit en tant que garante des droits fondamentaux. En ce sens, le cadre d'action prévu par la LECRIM conditionne le passage des enquêteurs, en soumettant leur activité à un ensemble de principes et d'exigences qui établissent un standard de garanties procédurales inhérent à l'État de droit.

Une enquête pénale peut affecter plusieurs droits fondamentaux tels que la liberté personnelle (art. 17 CE), la vie privée (art. 18.1 CE), l'inviolabilité du domicile (art. 18.2 CE), le secret des communications (art. 18.3 CE) et également la liberté de circulation (art. 19 CE), l'autorité judiciaire déterminant sous les hypothèses de la loi l'adoption éventuelle de toute mesure affectant les droits susmentionnés, par conséquent, bien qu'il doive y avoir une autorisation légale permettant son adoption, cela n'est toutefois pas suffisant. Il est nécessaire que la mesure d'infraction soit suffisamment motivée de manière à exprimer l'argumentation factuelle et juridique qui détermine son adoption conformément aux principes de spécialité, d'adéquation, d'exceptionnalité, de nécessité et de proportionnalité. En d'autres termes, une infraction pénale doit faire l'objet d'une enquête (spécialité) qui, en tout état de cause, doit être suffisamment grave pour justifier l'adoption d'une telle mesure, qui sert l'objectif de l'enquête (pertinence ; SSTC 85/1994, 14 mars, FJ 3° ; 181/1995, 11 décembre, FJ 5° ; 49/1996, 26 mars, FJ 3° ; 54/1996, 26 mars, FJ 7° et 8° ; 123/1997, 1er juillet, FJ 4°) car les résultats ne peuvent être obtenus par d'autres mesures moins contraignantes pour les droits fondamentaux de la personne faisant l'objet de l'enquête, étant indispensables du point de vue du cas spécifique (exceptionnalité et nécessité) et enfin, seuls des faits graves et socialement transcendants avec des indications fortes justifient le sacrifice de droits fondamentaux clés au risque d'assister à une situation d'impunité pénale (proportionnalité, STC 49/1999, 5 avril, FJ 7°).

Il est clair que la demande de limitation des droits fondamentaux que l'unité de police initie pour enquêter est soumise aux exigences de justification susmentionnées, de telle sorte que, face à un acte criminel en cours d'enquête, il existe un "mur" qui doit être franchi par une autorisation judiciaire afin de pouvoir poursuivre l'enquête. En aucun cas, une demande policière ne peut être faite à des fins prospectives (STS 822/2022, 18 octobre, Chambre II (Rapporteur : M. Palomo del Arco) , FJ 1º.3. a)), c'est-à-dire que sans un délit préalable indiscutablement justifié, il n'est même pas concevable d'exécuter une demande visant à obtenir une décision judiciaire qui porte atteinte à un droit fondamental. Par conséquent, il est clair que les forces de police sont là pour enquêter selon des paramètres précis et des limites claires, et bien que la clandestinité de l'enquête soit précise, sa destination finale est d'émerger dans un procès public dans le plein respect du droit de la défense et avec l'objectif clair de satisfaire les exigences de la "sécurité publique" (STC 175/1999 du 30 septembre, FJ 7º ou STC 86/2014, du 29 mai FJ 4º), quelque chose qui contraste avec la tâche des services secrets où les services secrets, dans l'intérêt de la protection de la "sécurité nationale", des informations sont recueillies auprès de personnes physiques ou morales, nationales ou étrangères, informations qui sont classifiées et qui ne sont certainement pas destinées à être diffusées publiquement devant un organe de poursuite pour en déduire une responsabilité pénale et sans que des notions telles que "contradiction", "défense", "suspect" ou "accusé" n'aient de substance propre, étant donné que leur travail n'a rien à voir avec l'enquête criminelle.

Cependant, malgré ce qui précède, les champs d'action des forces de police et des

services secrets sont communs. Le crime organisé, le terrorisme, l'immigration clandestine... constituent une menace simultanée pour la "sécurité publique" et la "sécurité nationale", de telle sorte que.. :

La criminalité organisée est une menace pour la sécurité qui se caractérise par sa finalité essentiellement économique, son effet de sape sur les institutions politiques et sociales, sa nature transnationale et son opacité. Les groupes et organisations criminels déguisent leurs opérations illégales en activités légitimes et s'appuient de plus en plus sur les technologies numériques, telles que les crypto-monnaies et le dark web. Outre sa dimension économique, la criminalité organisée a un potentiel de déstabilisation pertinent. Ses structures s'adaptent à l'environnement géostratégique et ont un impact sur la gouvernance, la paix sociale et le fonctionnement normal des institutions. En ce qui concerne la grande criminalité, des activités telles que l'exploitation des enfants ou la traite à des fins d'exploitation sexuelle ciblent des groupes vulnérables et portent gravement atteinte aux droits de l'homme. La contrebande, la cybercriminalité, le trafic de drogue, d'armes et d'espèces sauvages, ainsi que la corruption constituent des menaces tangibles pour la sécurité nationale. La convergence entre les groupes terroristes et les réseaux de criminalité organisée s'accroît. Les modes d'organisation de plus en plus décentralisés de ces acteurs criminels favorisent leur coopération et facilitent le financement du terrorisme (Stratégie de sécurité nationale (2021), pp. 64-65).

Il va sans dire que, compte tenu de ce qui précède, il est nécessaire que nos services secrets et les forces de police collaborent à une activité qui pourrait matériellement coïncider en termes de faits et de sujets, d'où sa nature clairement concentrique lorsqu'il s'agit, entre autres, du terrorisme, de la criminalité organisée ou des deux. À ce stade, une question se pose clairement : que se passe-t-il lorsque le CNI, grâce à ses écoutes, a connaissance d'un acte criminel qui pourrait faire l'objet d'une enquête en raison de son imminence ?

Il est clair qu'il n'existe pas de système de vases communicants légalement réglementé pour formaliser la transmission d'informations lorsque le CNI a connaissance de la commission d'actes criminels (Sánchez Barrilao, 2011, p. 61), étant donné que la loi 11/2002, du 6 mai, relative à la coopération avec les forces de sécurité ne contient pratiquement aucune référence, à l'exception d'aspects spécifiques tels que l'art. 9.2 d), qui attribue au SED le maintien et le développement de la "collaboration avec les services d'information des Forces et Corps de Sécurité de l'Etat, et les organes de l'administration civile et militaire, en rapport avec les objectifs d'intelligence". C'est ici qu'entre en jeu ce que nous avons précédemment qualifié de *" construction parallèle "*, en tant qu'expression de la configuration d'une affaire pénale par une force de police dissimulant l'origine de la source qui l'alimente (Reid, 2015, p. 427) et qui pourrait nécessairement être liée à des informations obtenues par une agence de renseignement, devant construire des éléments de preuve circonstancielle parallèles destinés à être le manteau qui cache la genèse de l'information originale, ce qui nous oblige à voir comment nous devrions traiter le matériel de renseignement en tant qu'initiateur ou moteur d'une enquête de police criminelle.

En principe, il faut partir de ce qui est dit dans le STS 746/2022, du 21 juillet, Chambre II, (Rapporteur : Mme Polo García) qui signale :

"Comme nous l'avons dit dans l'arrêt cité par la Chambre - 312/2021, du 13 avril -

les accusés n'ont pas le droit de divulguer le contenu et l'étendue des collaborations policières internationales. *Les enquêtés faisant l'objet d'une procédure pénale n'ont pas le droit de divulguer les points d'affectation de la police, ni l'identité des informateurs, ni les informations recueillies grâce à des techniques criminelles qui perdraient leur efficacité si elles étaient massivement divulguées. Il n'y a pas de droit à connaître les outils et matériels spécifiques dont disposait la police pour l'enquête et qui pourraient être rendus inefficaces pour des interventions futures.* Il n'y a pas non plus de droit à connaître les enquêtes sur d'autres crimes qui pourraient être attribués aux mêmes suspects mais qui sont encore en cours de confirmation policière, encore moins si l'on considère que, le cas échéant, ils devraient faire l'objet d'une procédure pénale distincte (art. 17.1 de la LECRIM). Il est également inacceptable que des enquêtes qui n'affectent même pas les personnes poursuivies et qui pourraient ruiner d'autres actions policières de poursuite obligatoire de la criminalité soient connues". (FJ 3.3).

L'origine de l'arrêt précédent était due au refus de l'organe judiciaire chargé des poursuites d'accepter le témoignage d'agents américains de la DEA qui avaient fourni des informations à la police nationale, laquelle avait mené une enquête sur les stupéfiants qui s'était soldée par une condamnation. Il convient de noter que l'arrêt précédent n'était pas nouveau ; notre Haute Cour avait déjà clairement indiqué que "...lorsque des services de renseignement étrangers fournissent des données aux forces et organes de sécurité espagnols, *l'exigence que la source de connaissance ait également besoin de ses propres sources de connaissance ne fait pas partie du contenu du droit à un procès assorti de toutes les garanties...*" (STS 445/2014, du 29 mai, Chambre II, Rapporteuse : Mme Ferrer García FJ 2º ; STS 884/2012, du 12 novembre, de la Chambre II, Président : M. Marchena Gómez FJ 8). Nous obtenons donc une première solution partielle : les services de renseignement étrangers peuvent fournir sans problème leurs sources à nos forces de police pour qu'elles puissent commencer à enquêter. Leur origine, en somme, n'est pas pertinente et, par conséquent, la DEA (ou le FBI, ou toute autre force de police étrangère) pourrait recevoir des informations de sa propre agence de renseignement (CIA, NSA... ou son service de renseignement) et les transmettre aux agences de police pour entamer une affaire pénale dans notre pays, sans entrer dans le débat sur l'assouplissement des normes juridiques pour les obtenir, puisqu'il n'y a pas de droit à débattre des sources de l'information, étant donné qu'il n'est pas nécessaire de les connaître pour mettre en place une procédure régulière.

La question de la transmission aux forces de sécurité par le CNI des informations qu'il a pu obtenir à la suite de ses écoutes téléphoniques ou de ses perquisitions nécessite des éclaircissements supplémentaires et est en fait une question abordée dans la jurisprudence qui nie que ses fonctions aient un rapport avec l'enquête pénale (SSTS 1140/2010, du 29 décembre, de la Chambre II (Rapporteur : M. Berdugo Gómez de la Torre) ; 1094/2010, du 10 décembre, de la Chambre II (Rapporteur : M. Marchena Gómez)). Et sur ce point, encore une fois, la méthodologie procédurale différente requise pour une interception téléphonique, par exemple, selon qu'elle est demandée par le CNI ou par un service de police, est qu'ils n'ont en commun que la nécessité d'une autorisation judiciaire, rien de plus.

Les arguments ne manquent pas pour justifier le fait que des informations obtenues par le CNI en violation d'un droit fondamental, et dans des conditions procédurales

propres - et non procédurales - avec une autorisation judiciaire, peuvent servir de source pour l'ouverture d'une affaire pénale avec une éventuelle communication aux forces de police.

Tout d'abord, il existe *un principe d'unité d'action entre la police et les services de renseignement*, imposé par les stratégies de sécurité nationale qui sont dictées comme cadre d'action (art. 4.3 LSN). Ainsi :

Dans les domaines traditionnels de la sécurité, l'adaptation à la nature changeante des menaces - conflits armés, terrorisme, criminalité organisée, prolifération, flux migratoires irréguliers, activités de renseignement - est une caractéristique constante de l'*action des différents acteurs de la sécurité nationale.* Ces phénomènes devenant de plus en plus transnationaux, *la nécessité d'une action concertée* à tous les niveaux *s'intensifie*. Les liens étroits qui existent souvent entre plusieurs de ces menaces font qu'il est nécessaire de les aborder à partir de cadres stratégiques et opérationnels larges, en vertu *du principe de l'unité d'action.* Le présent rapport montre que cette approche est déjà pleinement valable dans la réponse de l'Espagne aux défis classiques en matière de sécurité (Estrategia de Seguridad Nacional, 2013, p. 145).

Il est difficile, au risque de mettre en danger la collectivité, d'admettre un travail configuré dans des compartiments étanches, et c'est ainsi que la LSN impose cette " unité d'action " (art. 4.2), rappelant à l'art. 9.2 que " Les *Services de Renseignement et d'Information de l'Etat*, conformément à l'étendue de leurs compétences, soutiendront en permanence le Système de Sécurité Nationale, en fournissant des éléments de jugement, d'information, d'analyse, d'études et de propositions nécessaires pour prévenir et détecter les risques et les menaces *et contribuer à leur neutralisation* ". Par conséquent, l'exigence d'un sens convergent prend nécessairement la forme d'une coopération entre les agences ("Services") afin de répondre aux exigences visant à prévenir les risques ("contribuer à leur neutralisation"). En résumé, la communication d'informations est un élément clé pour contribuer à neutraliser les risques qui se présentent.

Deuxièmement, la communication pourrait être justifiée par l'*obligation de dénoncer les actes criminels ou leur commission imminente* par quiconque en est témoin, conformément à l'article 262 de la LECRIM (De la Oliva Santos 2006, p. 164), à commencer par le magistrat de la Cour suprême qui a autorisé l'interception des communications ou l'entrée au domicile du CNI (López Alafranca, 2014, p. 135). 164) à partir du magistrat du siège qui a autorisé l'interception de communications ou la pénétration dans le domicile du CNI (López Alafranca, 2014, p. 135) et également en vertu de l'exigence de la responsabilité pénale (407 et 408 CP) lorsqu'il s'agit d'agents de police qui peuvent fournir des services au CNI. La connaissance par le juge de l'évolution de la mesure autorisée doit nécessairement découler de la nécessité d'étendre les mesures limitant les droits fondamentaux auxquelles le CNI peut s'intéresser, car il n'est pas possible que l'organe d'autorisation ne connaisse pas les faits, à moins qu'une autorisation "aveugle" soit admise comme un "chèque en blanc" et sans contrôle successif, ce qui n'est pas possible puisque la loi prévoit une telle extension "en cas de nécessité" (art. 2 d) de la loi 2/2002), une nécessité qui devrait être justifiée par les faits résultant de la mesure initialement convenue, afin de poursuivre les mesures restrictives.

La thèse ne peut être acceptée, sans préjudice de sa validité, selon laquelle le fait que les agents du CNI ne soient pas considérés comme des autorités (art. 5.4 de la loi

11/2002) empêche l'obligation de dénoncer les délits (Lanz Muniain, 2023, p. 34), mais l'obligation imposée par l'article 262 de la LECRIM à ceux qui "en raison de leurs fonctions, professions ou métiers" ont connaissance de l'acte délictueux détermine qu'il est indifférent qu'ils soient ou non une autorité ou son agent, puisqu'ils ont connaissance de l'acte par leur profession et qu'ils doivent le dénoncer. Cependant, cette communication a été approuvée par la Cour Suprême elle-même lorsqu'elle affirme que "Par conséquent, la fonction légale de ce service n'est pas d'enquêter sur des crimes spécifiques, sans préjudice du fait que si, au cours de leur travail, *ils découvrent* ou ont des indications d'actions criminelles, *ils en informent les organes policiers et judiciaires compétents*, mais - on insiste - leur activité ne vise pas directement à la découverte de crimes, ni n'est conditionnée par la commission préalable de l'un d'entre eux" (STS 1140/2010, du 29 décembre, de la Chambre II (Rapporteur : M. Berdugo Gómez Gómez). Berdugo Gómez de la Torre) FJ 9º) .

Troisièmement, *une hypothétique classification secrète ne peut couvrir l'impunité d'actes criminels* (López Alafranca, 2014, p. 136) qui, en revanche, doivent nécessairement être empêchés. De même, même dans le cas d'informations classifiées ("organisation et structure internes, moyens et procédures, personnel, installations, bases de données et centres de données, sources d'information et informations ou données pouvant conduire à la connaissance des matières susmentionnées..." ex art. 5.1 de la loi 11/2002), rien ne s'oppose à une procédure de déclassification des informations au niveau procédural, mais il s'agit d'une question sans rapport avec la communication elle-même qui, précisément, a pour limite l'information transmise dans laquelle le matériel qui doit être déclassifié n'est pas divulgué (Pascual Sarria, 2007 p. 214).

Quatrièmement, c'est précisément la collecte d'informations par le CNI, si elle implique une violation de la confidentialité des communications ou une entrée dans le domicile, *qui est soutenue par une décision judiciaire nécessairement motivée par son effet nuisible* (SSTC 126/1995, 25 juillet, FJ 2 ; 139/1999, 22 juillet, FJ 2 ; dans le même sens, SSTC 290/1994, 27 octobre, FJ 31 ; 50/1995, 23 février, FJ 5 ; 41/1998, 23 février, FJ 34 ; 171/1999, 23 septembre, FJ 10 ; 8/2000, 8 janvier, FJ 4) ; 41/1998, du 24 février, FJ 34 ; 171/1999, du 27 septembre, FJ 10 ; 8/2000, du 17 janvier, FJ 4), ces mesures n'ont donc pas été convenues en dehors d'un schéma procédural ou sur un coup de tête en fonction de leurs besoins opérationnels, de sorte qu'il n'y a pas d'illégalité dans leur obtention et, par conséquent, ni dans leur communication pour l'ouverture d'une enquête pénale, enquête qui n'est pas contaminée.

À cet égard, l'aspect probatoire doit être distingué de la question proprement dite de la communication en vue de l'ouverture d'une procédure pénale. Il s'agit de questions différentes. Le matériel obtenu par le CNI n'est pas destiné à servir de preuve dans une procédure pénale, car c'est l'enquête policière elle-même qui doit remplir cette fonction, rappelant qu'il n'y a de "preuve illicite" (art. 11 LOPJ) que "lorsque les moyens utilisés pour l'obtenir sont constitutionnellement illégitimes" (STC 49/1999, 5 avril, FJ 12). Dans ce sens, le STS 1094/2010, du 10 décembre, dans son FJ 2 A nous rappelle que ".... Mais ce qui ne fait aucun doute, *c'est que l'existence d'une procédure pénale ultérieure dans laquelle le notitia criminis n'est pas étranger au fichier de sécurité traité par le CNI n'implique pas la transmutation de la fonctionnalité de ce fichier,* qui cesserait d'être ce qu'il est, s'éloignant de ses principes régulateurs, pour devenir un acte de procédure sine qua non du processus réel et, par conséquent, soumis aux règles générales régissant le principe de publicité".

Et c'est précisément la décision judiciaire d'autorisation qui nous empêche de parler d'une sorte de "corniche" illégale sur laquelle notre service de renseignement se déplacerait de manière risquée. Cependant, bien que nous ayons dit que le matériel de renseignement n'est pas destiné à la procédure pénale en tant qu'élément de preuve, il ne faut pas oublier que "et en ce qui concerne l'incorporation dans la procédure de preuves obtenues par les services de renseignement et qui se réfèrent à du matériel déclassifié, elle peut être évaluée de deux points de vue différents. Soit il agit dans la procédure pénale en tant que preuve documentaire, lorsqu'il s'agit d'une preuve présentant ces caractéristiques, soit il sert à mener l'enquête pénale par le biais du témoignage des auteurs" (STS 1140/2010, du 29 décembre, Chambre II (Rapporteur : M. Berdugo Gómez de la Torre) FJ 9º).

Cependant, les objections au système ne manquent pas, à commencer par les complexités que la présence des services secrets dans les procédures pénales pourrait impliquer (Hassemer, 2000, p. 114), de sorte qu'il pourrait y avoir une confusion, presque un mélange, qui rendrait indiscernables les fonctions de police et de collecte de renseignements (Orgis, 2011, p. 162). Ce ne serait pas bon pour les forces de police, ce ne serait pas bon pour les services secrets, et ce en vertu des différents paramètres d'action. D'autre part, l'obtention d'une mise sur écoute ou d'une visite domiciliaire par nos services secrets est soumise à une norme différente selon laquelle il faut justifier ses propres dangers extrêmes pour la sécurité nationale, qui n'ont peut-être rien à voir avec la commission d'un acte criminel. En résumé, c'est une chose si, au cours d'une opération de renseignement, on découvre un acte criminel grave ou dont la commission est imminente, ce qui doit nécessairement être communiqué ou signalé aux forces de police, et c'en est une autre si la procédure de demande et d'obtention d'une mise sur écoute ou d'une intrusion par les services secrets sert, en tant que raccourci procédural, à rechercher le crime lui-même, ce qui conduirait à l'inutilité du système de garanties procédurales constitutionnelles en ce qui concerne la limitation et la violation des droits fondamentaux.

Enfin, nous avons constaté précédemment que toutes les informations ne peuvent être connues, ce qui pourrait conduire, dans le cadre d'une procédure pénale, à la mise à l'épreuve des droits de la défense (art. 24.2 CE), puisque l'accès au dossier dans le cas du CNI est soumis à des restrictions et à une situation de classification qui contraste avec la mise à disposition des parties impliquées de tous les éléments de l'enquête pénale. En d'autres termes, la présence des services secrets et les informations qu'ils obtiennent dans le cadre d'une procédure pénale ne peuvent émerger aussi naturellement que dans le cadre d'une enquête policière. En résumé, tout le monde n'a pas accès à toutes les informations, ce qui signifie qu'il y a des éléments qui ne font pas l'objet d'une hypothétique stratégie de défense, soit d'une personne sous enquête, soit de tiers hors procédure dont les communications ou les adresses pourraient être affectées, qui resteront cachés, ce qui peut servir à remettre en question la pureté de la procédure et de la décision sur la responsabilité pénale.

5. CONCLUSIONS.

Il existe une relation concentrique entre la sécurité nationale et la sécurité publique dans la mesure où toutes deux reposent sur l'hypothèse de l'existence de menaces pour l'État de droit. Toutefois, les acteurs habilités à les protéger sont différents, les services secrets étant compétents pour la première et la police pour la seconde. En ce sens, des outils ont été mis en place pour prévenir les risques susmentionnés par l'attribution de mesures limitant les droits fondamentaux. Dans le cas des agences de sécurité publique (police d'État, régionale ou locale), leurs pouvoirs s'inscrivent dans le cadre de la procédure pénale avec des lignes directrices très rigoureuses pour la violation des droits grâce à la nécessité d'une autorisation judiciaire pour autoriser des activités invasives mais ordonnées par les forces de sécurité dans le cadre de la LECRIM. Le service de renseignement (CNI) n'a été habilité que relativement récemment à intercepter les communications et à pénétrer dans les domiciles par le biais d'une loi de contrôle judiciaire en 2002, mais nous ne pouvons pas affirmer que ses exigences coïncident avec celles de la LECRIM lorsqu'il s'agit de les accorder, de sorte que nous nous trouvons dans un système de deux poids, deux mesures en fonction du sujet qui agit.

Le concept de *construction parallèle* résulte d'une façon d'agir des forces de police qui reçoivent des informations de renseignement qui, d'une part, leur permettent de monter des dossiers criminels mais qui, d'autre part, compte tenu du fait qu'il existe une norme inférieure pour l'obtention d'informations de renseignement, sont obligées de dissimuler leur origine, en cherchant des procédures alternatives pour empêcher la source originale de faire surface et en permettant à la personne faisant l'objet de l'enquête de remettre en question leur acquisition en violant les procédures régulières. Cette question a été mise en évidence principalement en Amérique du Nord à la suite de l'effondrement du "mur" entre les activités de police et de renseignement avec les attentats du 11 septembre 2001, ce qui a suscité des doutes quant à l'utilisation des informations obtenues auprès de la Foreign Intelligence Court (FISA Court) dont les mandats de surveillance à une agence de renseignement fournissent des informations qui peuvent ensuite être utilisées par les forces de police qui ont pu éviter d'avoir à justifier d'une cause probable devant une instance judiciaire pour mener à bien leurs enquêtes. En d'autres termes, il semble qu'il s'agisse d'une sorte de raccourci opérationnel qui génère des doutes, des doutes qui nous affectent également quant à l'utilisation possible des informations résultant d'une autorisation du juge de la Cour suprême à la CNI en dehors d'une écoute téléphonique, en dehors d'une pénétration dans un domicile. En ce sens, il existe une série d'exigences qui motiveraient la communication d'un acte criminel résultant de la pratique d'une procédure restrictive des droits fondamentaux par nos services secrets aux services de police, qui pourrait bien être l'obligation générale de dénonciation prévue à l'article 262 de la LECRIM. Mais une unité d'action élémentaire dans la prévention des menaces qui affectent conjointement la sécurité publique et nationale exige la coopération entre les services et l'échange d'informations. Personne ne doute de la nécessité de communiquer et d'alerter, indépendamment de l'éventuelle classification secrète de l'information, classification qui ne peut couvrir le silence face à un acte criminel ni permettre qu'il reste impuni. Il existe d'ailleurs un processus de déclassification à cet effet.

Notre Cour suprême a déclaré que lorsqu'un service de renseignement étranger envoie une confidence qui sert à ouvrir une affaire pénale, il n'y a pas de droit à connaître la source de la source, et qu'il n'est donc pas nécessaire, ni approprié, de dissimuler l'origine ou la source de la connaissance par l'agence de police. Dans le cas d'une

communication du CNI à une force de sécurité publique, notre Haute Cour approuve également, bien que de manière isolée, la communication d'un acte criminel sans entrer dans la question de savoir si l'information est classée secrète ou non, ce qui signifie que ni la dissimulation ni le développement de stratégies alternatives, qui pourraient compromettre la procédure pénale, ne semblent avoir de sens. Il n'y a donc pas de place pour une *construction parallèle*, sans préjudice du fait que la présence de services secrets dans les procédures pénales soulève des questions qui, pour être résolues, nécessiteront une réforme du système conçu par la loi 2/2002 du 6 mai.

6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Aba Catoira, A. (2020). Accountability and intelligence services. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Tirant lo Blanch.

Alfonso Rodríguez, A. J. (2023). Gouvernance démocratique et responsabilité : contrôle judiciaire des activités de renseignement (ODD 16.6). *Revista de Derecho UNED*, (31).

Alfonso Rodríguez, A. J. (2024). Interception des communications téléphoniques, sécurité(s) et garanties procédurales. *Revista Ciencia Policial*, (182).

Arrieta, G. (2025). Balancing the scales : Amici curiae as special masters in the shadow of FISA. *California Western Law Review, 61*(1), Article 6. https://scholarlycommons.law.cwsl.edu/cwlr/vol61/iss1/6

Beck, U. (2006). *La sociedad del riesgo : Hacia una nueva modernidad.* Paidós Ibérica.

Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. *The Yale Law Journal, 131*(2). http://www.yalelawjournal.org/author/simon-chin

De la Oliva Santos, A. (2006). *Écrits sur le droit, la justice et la liberté.* Editorial UNAM, Instituto de Investigaciones Jurídicas.

Donohue, L. K. (2021). L'évolution et la jurisprudence de la Foreign Intelligence Surveillance Court et de la Foreign Intelligence Surveillance Court of Review. *Harvard National Security Journal, 12.*

Gómez Colomer, J. L. (2006). Système accusatoire, processus accusatoire et principe accusatoire : une réflexion sur le modèle de poursuite pénale appliqué aux États-Unis d'Amérique. *Revista Poder Judicial*, (Spécial XIX).

Hassemer, W. (2000), Criminal proceedings without data protection ? In C. M. Romeo Casabona (Ed.), *La insostenible situación del derecho penal (*pp. 103-128). Comares.

Herbón Costas, J. J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional : La pandemia por covid-19 y la necesidad de una urgente reforma. *Revista Española de Derecho Constitucional, 121.* https://doi.org/10.18042/cepc/redc.121.05

Lanz Muniain, V. (2023). El CNI un servicio de inteligencia y seguridad : Panorama normativo. *Revista Española de Derecho Militar, (*119).

López Alafranca, M. (2014). Mais qui surveillera les gardiens ? *Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales,* (92).

Orgis, M. (2011). Intelligence-led and intelligence-guided operations : The best option for combating pre-eminent threats. Dans J. Fernández Rodríguez, D. Sanso-Rubert

Pascual, J. Pulido Grajera, et R. Monsalve (Eds.), *Intelligence issues in contemporary society (*pp. 143-166). Ministère de la défense.

Pascual Sarria, F. (2007). El control judicial a la interceptación de las comunicaciones : Especial referencia al control judicial previo a las intervenciones del Centro Nacional de Inteligencia. *Revista Española de Derecho Militar, (*89).

Pinto Cebrián, F. (2019). *Manuel d'intelligence et de contre-intelligence (terrorisme et contre-terrorisme)*. Amabar.

Reid, L. (2015). NSA and DEA intelligence sharing : Why it is legal and why Reuters and the Good Wife got it wrong (Partage de renseignements entre la NSA et la DEA : pourquoi c'est légal et pourquoi Reuters et The Good Wife se sont trompés). *SMU Law Review, 68*(2), article 5.

Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court : An empirical perspective. *Northwestern University Law Review, 101*(1).

Sánchez Barrilao, J. F. (2011). Prévention et renseignement : le Centre national de renseignement et la communauté du renseignement face au terrorisme, au crime organisé et à l'immigration illégale. *Revista Ejército,* (846).

Sánchez Ferro, S. (2020). Mission impossible ? Une tentative de compréhension juridique du monde de l'espionnage en Espagne. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 159-207). Tirant lo Blanch.

Sobel, A. X. (2023). Procedural protections in a secret court : FISA amici and expanding appellate review of FISA decisions. *University of Pennsylvania Law Review, 172* [Note : Corrected "Pennsylvania" to "Pennsylvania". Numéros de page ou d'article manquants].

Stein, R., Mondale, W. et Fisher, C. (2016). No longer a neutral magistrate : The Foreign Intelligence Surveillance Court in the wake of the war on terror. *Minnesota Law Review, 100.* https://scholarship.law.umn.edu/faculty_articles/564

Zaffaroni, E. R. (2006). *El enemigo en el Derecho Penal*. Dykinson.