



Revista Científica del Centro Universitario de la Guardia Civil

Revista **Lógos** Guardia Civil

Version
Français

Vol. 3 Núm. 2 (2025)
juin

RÉSUMÉ

I.- COLLABORATIONS

Coopération entre les services répressifs et les poursuites pénales : une construction parallèle ?
Adriano J. Alfonso Rodríguez

II.- TRAVAUX DE RECHERCHE

L'Espagne face à la désinformation : défis hybrides et réponses conventionnelles
Juan Francisco Adame Hernández

L'intelligence en point de mire : de la théorie classique à une nouvelle approche de la mise en œuvre à l'ère numérique · Paula Castro Castañer

Hacktivisme : de la protestation sociale à l'instrumentalisation de l'État · Josué Expósito Guisado
Protection internationale et souveraineté : l'équilibre délicat entre les droits individuels et la sécurité nationale · Alejandro Gómez García

La guerre contre la drogue de Nixon et l'essor de la surveillance virtuelle des frontières aux États-Unis · J. Luigi M. Kunz Saponaro

La violence sexuelle des étrangers à Madrid et à Barcelone : une analyse situationnelle
Francisco Pérez-Fernández/ Heriberto Janosch/ Enrique López López/ Francisco López-Muñoz
Drogues et conduite : "Tolérance zéro". Méthodologie du rapport salivaire du laboratoire Synlab et critères d'approbation de l'entité nationale d'accréditation
Juan Carlos Rodríguez Bello

Protéger les infrastructures sous-marines essentielles et renforcer la sécurité de la mer Baltique : l'opération Baltic Sentry de l'OTAN · Mónica Román González

Le capital intellectuel dans l'institution de la Garde civile et sa contribution à l'économie sociale
Virginia Belén Subiris Moriel

III.- ANALYSE DE LA JURISPRUDENCE

Revue de Jurisprudence 2ème Chambre Cour Suprême · Javier Ignacio Reyes López



MINISTERIO
DEL INTERIOR





Edita :

Ministère de l'Intérieur. Secrétariat général technique. Madrid.

Catalogue des publications de l'administration générale de l'État :
<https://cpage.mpr.gob.es>.

Logos Guardia Civil Magazine

Revue scientifique du Centro Universitario de la Guardia Civil (Centre universitaire de la Garde civile)

Date d'édition : juin 2025

OPIN (papier) : 126-23-018-2

ONPIC (en ligne) : 126-23-019-8

Dépôt légal : M-3619-2023

ISSN : 2952-3249

ISSN en ligne : 2952-394X

Entité responsable :

Centre universitaire de la Guardia Civil

Domaine de recherche

Paseo de la Princesa, s/n

28300 Aranjuez (Madrid)

e-mail : investigacion@cugc.es

Conception et mise en page :

Bureau du domaine de la recherche

Les opinions exprimées dans cette publication relèvent de la seule responsabilité des auteurs.

La publication de cette revue et sa diffusion sont effectuées conformément aux politiques d'accès libre à la production scientifique. Ainsi, et dans le but de mettre la connaissance à la disposition de la société dans son ensemble, cette revue publie tous les articles et autres contenus numériques gratuitement sous une licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) (<https://creativecommons.org/licenses/by-nc-nd/4.0/>).

DIRECTEUR

Félix Blázquez González. Lieutenant général de la Garde civile. Directeur de la CUGC.

RÉDACTEUR EN CHEF

Blas Guillamón Campos. Lieutenant-colonel de la Garde civile. CUGC.

SECRÉTAIRE

Oliver Cadenas Roldán. Commandant de la Guardia Civil CUGC.

COMITÉ ÉDITORIAL

Félix Blázquez González. Lieutenant général de la Garde civile. Dtor CUGC.

Blas Guillamón Campos. Lieutenant-colonel de la Garde civile. CUGC.

Carlos Fernández Liesa. Professeur de droit international public et de relations internationales. Délégué de l'UC3M à la CUGC.

Ana M^a Garrocho Salcedo. Vice-doyenne des études internationales - Droit UC3M.

Dr Francisco López Muñoz. Professeur de pharmacologie. Vice-recteur pour la recherche et les sciences - UCJC.

Clara Sainz de Baranda Andujar. Directrice de l'Institut d'études de genre - UC3M.

Manuel Díaz Martínez. Professeur de droit procédural - UNED.

Jordi Gimeno Beviá. Vice-doyen pour la recherche et l'internationalisation. Faculté de droit - UNED.

Ricardo Cuevas Campos. Vice-recteur de la politique scientifique - UCLM

Dr. Amaya Arnáiz Serrano. Directrice adjointe de l'Institut Alonso Martinez de la justice et du contentieux - UC3M.

Dr. Cástor M. Díaz Barrado. Professeur de droit international public et de relations internationales - URJC.

Carlos Berbell Bueno. Journaliste. Directeur du journal Conflegal.

Oliver Cadenas Roldán. Commandant de la Guardia Civil. Secrétaire.

COMITÉ SCIENTIFIQUE

Félix Blázquez González. Lieutenant général de la Garde civile. Directeur de la CUGC.

Anselmo del Moral Torres. Colonel de la Guardia Civil. Directeur exécutif de la CUGC.

Dr. Eduardo Martínez Viqueira. Chef général du commandement personnel de la Guardia Civil.

Jacobo Barja de Quiroga López. Président de la 5ème chambre de la Cour suprême.

Julián Sánchez Melgar. Juge. Deuxième chambre de la Cour suprême.

Juan Díez Nicolás. Professeur de sociologie. Membre de l'Académie royale des sciences morales et politiques.

Juan Aparicio Barrera. Rédacteur en chef du magazine Logos Science & Technology. Colombie.

Pablo Morenilla Allard. Professeur de droit procédural - UCLM.

Jacobo Dopico Gómez-Aller. Professeur de droit pénal - UC3M.

Fernando Bandrés Moya. Professeur de médecine légale - UCM.

Blas Guillamón Campos. Lieutenant-colonel de la Garde civile. CUGC.

Oliver Cadenas Roldán. Commandant de la Guardia Civil. Secrétaire.

Site officiel Logos Guardia Civil Magazine

<https://revistacugc.es>



Site officiel de la CUGC

<https://www.cugc.es>





INDEX

INTRODUCTION	9
--------------------	---

I.- COLLABORATIONS

Coopération entre les services répressifs et les poursuites pénales : une construction parallèle ? 13

Adriano J. Alfonso Rodríguez

II.- TRAVAUX DE RECHERCHE

L'Espagne face à la désinformation : défis hybrides et réponses conventionnelles 37

Juan Francisco Adame Hernández

L'intelligence en point de mire : de la théorie classique à une nouvelle approche de la mise en œuvre à l'ère numérique..... 71

Paula Castro Castañer

Hacktivism : de la protestation sociale à l'instrumentalisation de l'État 101

Josué Expósito Guisado

Protection internationale et souveraineté : l'équilibre délicat entre les droits individuels et la sécurité nationale 123

Alejandro Gómez García

La guerre contre la drogue de Nixon et l'essor de la surveillance virtuelle des frontières aux États-Unis 147

J. Luigi M. Kunz Saponaro

La violence sexuelle des étrangers à Madrid et à Barcelone : une analyse situationnelle..... 171
--

Francisco Pérez-Fernández / Heriberto Janosch / Enrique López López / Francisco López-Muñoz

Drogues et conduite : "Tolérance zéro". Méthodologie du rapport salivaire du laboratoire Synlab et critères d'approbation de l'entité nationale d'accréditation. 197

J uan Carlos Rodríguez Bello

Protéger les infrastructures sous-marines essentielles et renforcer la sécurité de la mer
Baltique : l'opération Baltic Sentry de l'OTAN..... 221

Mónica Román González

Le capital intellectuel dans l'institution de la Garde civile et sa contribution à l'économie
sociale 257

Virginia Belén Subiris Moriel

III.- ANALYSE DE LA JURISPRUDENCE

Revue de Jurisprudence 2ème Chambre Cour Suprême 295

Javier Ignacio Reyes López



INTRODUCTION

Cher lecteur,

Nous sommes heureux de vous accueillir dans le cinquième numéro de notre revue Logos Guardia Civil, éditée par le Centre universitaire de la Garde civile. Ce nouveau numéro rassemble une sélection d'articles qui abordent, sous différents angles et dans différentes disciplines, certains des défis les plus urgents dans le domaine de la sécurité, tant au niveau national qu'international.



Nous ouvrons ce numéro avec la collaboration de M. Adriano J. Alfonso Rodríguez, docteur en droit et professeur de droit et de criminologie à l'UNED, qui nous offre une réflexion opportune sur la « Coopération entre les agences de sécurité et les processus d'intégration régionale en Amérique latine ».

Dans la section des articles de recherche, Juan Francisco Adame Hernández, directeur de la stratégie, de la communication et de la promotion de la Casa Árabe, nous présente « L'Espagne face à la désinformation : défis hybrides et réponses conventionnelles », une étude rigoureuse sur les risques de la désinformation pour la sécurité de l'État.

Paula Castro Castañer, experte en sécurité et doctorante en sciences médico-légales à l'université d'Alcalá, nous présente « L'intelligence dans le collimateur : de la théorie classique à la mise en œuvre à l'ère numérique », une approche critique de la perception sociale des services de renseignement.

Le travail de Josué Expósito Guisado, sergent de la Garde civile et doctorant à l'université Pablo de Olavide, intitulé « Hacktivisme : de la protestation sociale à l'instrumentalisation étatique », analyse les limites entre l'action numérique et l'illégalité pénale.

Alejandro Gómez García, capitaine de la Garde civile et titulaire d'un master en gestion opérationnelle de la sécurité, approfondit la question de la « Protection internationale et souveraineté : le difficile équilibre entre droits individuels et sécurité nationale », un sujet très sensible en droit international.

Don Johannes Luigi Maria Kunz Saporano, chercheur doctoral à l'université Carlos III de Madrid, analyse dans son article « La guerre de Nixon contre la drogue et l'essor de la surveillance virtuelle des frontières aux États-Unis » la transformation de la sécurité

aux États-Unis, en soulignant comment les politiques mises en œuvre pendant la « guerre contre la drogue » ont donné lieu au développement de systèmes sophistiqués de contrôle des frontières s'appuyant sur des technologies de pointe.

L'équipe formée par Francisco Pérez-Fernández, Heriberto Janosch, Enrique López López et Francisco López-Muñoz présente « La violence sexuelle exercée par des inconnus à Madrid et Barcelone : une analyse situationnelle », une étude qui apporte des informations pertinentes sur la répartition géographique et les schémas comportementaux des agressions sexuelles en milieu urbain.

Juan Carlos Rodríguez Bello, caporal de la brigade routière de la Garde civile, expert universitaire en délinquance routière et expert judiciaire en documentoscopie à l'UNED, signe l'article « Drogues et conduite : tolérance zéro. Méthodologie du rapport salivaire du laboratoire Synlab et critères d'homologation de l'Entité nationale d'accréditation », qui traite des normes scientifiques et juridiques en matière de détection de substances.

Mónica Román González est doctorante au programme de sciences politiques, administration et relations internationales de l'université Complutense de Madrid. Elle nous propose une analyse stratégique dans « La protection des infrastructures sous-marines critiques et le renforcement de la sécurité de la mer Baltique : l'opération Baltic Sentry de l'OTAN », soulignant l'importance de la coopération internationale dans les scénarios maritimes.

Enfin, Virginia Belén Subiris Moriel, doctorante à l'université Rey Juan Carlos, programme Sciences sociales et juridiques, clôt le numéro avec « Économie sociale : la contribution de l'institution de la Garde civile à travers son capital intellectuel », un article qui explore la valeur du partage des connaissances et l'engagement institutionnel en faveur du développement social.

D'autre part, la section consacrée aux revues jurisprudentielles compte cette fois-ci une nouvelle contribution de Javier Ignacio Reyes López, magistrat juge doyen d'Alcalá de Henares, qui analyse des arrêts importants de la deuxième chambre de la Cour suprême.

Le comité de rédaction tient à remercier sincèrement les auteurs pour leur rigueur et leur engagement, ainsi que les évaluateurs externes pour leur travail indispensable. Nous espérons que cette nouvelle édition vous intéressera et contribuera à la connaissance, à la réflexion et à l'amélioration continue dans le domaine de la sécurité.

Félix Blázquez González
Directeur du CUGC



I.- COLLABORATIONS



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.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

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 habilitier 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.

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. 149.1.29^a CE). L'art. 149.1.29^a CE ou la propriété exclusive de l'État sur la "sécurité publique" (art. 149.1.29^a 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 7^o 86/2014, du 29 mai, FJ 4^o ou 55/1990, du 28 mars, FJ 5^o). 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 1^o), 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 7^o), 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 États-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 comparait 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 4^o) 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 1°.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 7° ou STC 86/2014, du 29 mai FJ 4°), 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 9°).

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.



II.- TRAVAUX DE RECHERCHE



Article de recherche

L'ESPAGNE FACE A LA DESINFORMATION: DEFIS HYBRIDES ET REPONSES CONVENTIONNELLES

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

Juan Francisco Adame Hernández

Directeur de la stratégie, de la communication et de la promotion de la Casa Árabe

Master en sécurité internationale - haute gestion

Master en études avancées en communication politique

Reçu le 08/04/2025

Accepté le 03/06/2025

Publié le 27/06/2025

Citation recommandée : Adame, J. F. (2025). L'Espagne face à la désinformation : défis hybrides et réponses conventionnelles. *Revista Logos Guardia Civil*, 3(2), pp. 37-70.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

L'ESPAGNE FACE A LA DESINFORMATION : DÉFIS HYBRIDES ET RÉPONSES CONVENTIONNELLES

Résumé: INTRODUCTION. 2. DÉSINFORMATION, POST-VÉRITÉ ET FAKE NEWS. 2.1. Concepts et définitions. 3. STRATÉGIES HYBRIDES ET ZONE GRISE. 3.1 Manipulation et interférence de l'information étrangère (FIMI). 4. DOMINATION COGNITIVE ET DÉSINFORMATION. 5. CONSTRUCTION DE RÉCITS ET DE CADRES. 5.1. Mise en œuvre. 5.2. Impact des récits et des cadres dans le domaine cognitif. 6. ÉVOLUTION DE LA DÉSINFORMATION. 7. MESURES ET OUTILS ACTUELS DE LUTTE CONTRE LA DÉSINFORMATION EN ESPAGNE. 7.1. Procédure d'action contre la désinformation. 8 CONCLUSIONS. 9 RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Dans l'environnement géopolitique actuel, caractérisé par la prolifération des technologies de l'information et l'interconnexion mondiale, la **désinformation s'est imposée comme une menace multidimensionnelle** qui compromet les structures de sécurité nationale et la cohésion sociale des États. Cet article analyse la **réponse institutionnelle et stratégique de l'Espagne à la désinformation**, en l'inscrivant dans le contexte plus large des stratégies hybrides et de l'**interférence et de la manipulation de l'information étrangère (FIMI)**.

L'étude aborde des concepts clés tels que la *désinformation*, la *post-vérité* et la *zone grise*, en les reliant à l'**évolution doctrinale des stratégies hybrides au sein de l'Union européenne**. Une attention particulière est accordée au **domaine cognitif** et aux mécanismes de construction narrative et aux cadres interprétatifs utilisés pour façonner et déformer la perception du public. La dernière partie propose une **évaluation critique des principales mesures adoptées par l'Espagne pour lutter contre la désinformation**, en évaluant leur cohérence, leur mise en œuvre et leur efficacité dans un paysage de menaces en constante évolution.

Resumen: En el actual entorno geopolítico, caracterizado por la proliferación de tecnologías de la información y la interconexión global, **la desinformación se ha consolidado como una amenaza multidimensional** que compromete las estructuras de seguridad nacional y la cohesión social de los Estados. Este artículo analiza **la respuesta institucional y estratégica de España frente a la desinformación**, enmarcándola dentro del contexto más amplio de las estrategias híbridas y de la **interferencia y manipulación informativa extranjera (FIMI)**.

El estudio aborda conceptos clave como *desinformación*, *posverdad* y *zona gris*, vinculándolos con la **evolución doctrinal de las estrategias híbridas en el seno de la Unión Europea**. Se presta especial atención al **dominio cognitivo** y a los mecanismos de construcción de narrativas y marcos interpretativos empleados para moldear y distorsionar la percepción pública. La última sección ofrece una **evaluación crítica de las principales medidas adoptadas por España para contrarrestar la desinformación**, valorando su coherencia, aplicación y eficacia en un panorama de amenazas en constante transformación.

Mots-clés : Désinformation, *Fake news*, stratégies hybrides, domaine cognitif, récits.

Palabras clave: Desinformación, *Fake news*, Estrategias híbridas, Dominio cognitivo, Narrativas.

ABBREVIATIONS

CIS : Centro de Investigaciones Sociológicas (Centre de recherche sociologique)

CNI : Centre national de renseignement

DESI : Indice de l'économie et de la société numériques

DHS : Département de la sécurité intérieure

SEAE/EEAS : Service européen d'action extérieure

ELISA : étude simplifiée à source ouverte

ENISA : Union européenne pour la cybersécurité

ESN : Stratégie de sécurité nationale

UE/EU : Union européenne

FIMI : Manipulation et interférence de l'information étrangère

FIJ : Fédération internationale des journalistes

INCIBE : Instituto Nacional de Ciberseguridad, cybersécurité.

MAEUEC : Ministère des Affaires étrangères, de l'Union européenne et de la Coopération

MPJRC : Ministère de la présidence, de la justice et des relations avec les tribunaux

OMS : Organisation mondiale de la santé

OTAN/NATO : Organisation du traité de l'Atlantique Nord/Organisation du traité de l'Atlantique Nord

1. INTRODUCTION

À l'ère du numérique, marquée par la diffusion rapide de l'information par les médias sociaux et les technologies de la communication, la désinformation est devenue une menace stratégique majeure. Ce phénomène, qui comprend les "*fake news*" et la "post-vérité", a acquis une importance sans précédent dans la sphère géopolitique, affectant à la fois la stabilité des systèmes politiques, la perception du public et la sécurité nationale. L'Espagne n'a pas été épargnée par ces défis et a dû faire face à des campagnes de désinformation qui, dans de nombreux cas, ont été utilisées comme des outils dans le cadre de stratégies hybrides plus larges.

La désinformation est souvent interprétée comme un phénomène en soi ou abordée de manière isolée ou décontextualisée (Lazer et al., 2018). Les stratégies dans lesquelles s'inscrit la désinformation sont relativisées, abstraites ou ignorées (MAEUEC, 2021). Obviant à la nécessaire approche multidisciplinaire (Wardle et Derakhshan, 2017) ou au besoin d'identifier les objectifs stratégiques que ces actions ou campagnes de désinformation poursuivent (Terán, 2019). Même lorsqu'il est fait référence aux stratégies hybrides et/ou à la zone grise, celles-ci ne sont généralement pas abordées en profondeur, étant reléguées à une simple mention (DSN, 2021). La désinformation, loin d'être un phénomène isolé, s'inscrit dans un cadre stratégique plus large, comprenant les stratégies hybrides et ce que l'on appelle la "zone grise" (OTAN, 2024), et en particulier la *manipulation de l'information étrangère et l'ingérence* (*Foreign Information Manipulation and Interference* - FIMI).

2. DÉSINFORMATION, POST-VÉRITÉ ET FAKE NEWS

La désinformation n'est pas un phénomène récent (Allcott et Gentzkow, 2017 ; Tandoc, Lim et Ling, 2018). Depuis que les sociétés ont commencé à s'organiser en structures hiérarchiques, les humains ont délibérément fabriqué et diffusé des histoires incorrectes et trompeuses (Burkhardt, 2017). Des tactiques de dénigrement politique dans la Rome antique aux stratégies de propagande pendant la Première et la Seconde Guerre mondiale (Posetti et Matthews, 2018), la désinformation a été utilisée pour manipuler et convaincre les autres. La désinformation a atteint des niveaux sans précédent, modifiant non seulement la perception du public, mais influençant aussi directement les processus politiques et sociaux à l'échelle mondiale. Cependant, comme le rappellent Julie Posetti et Alice Matthews dans leur compilation "*A Short Guide to History of Fake News and Disinformation*" (2018), la fabrication et la manipulation de l'information n'est pas un phénomène nouveau.

Ces dernières années, les médias, les campagnes politiques ou les débats sportifs (ou non sportifs) sur les réseaux sociaux ont été remplis de nouveaux concepts tels que les *fake news* (Tandoc, Lim & Ling, 2018), la post-vérité (McIntyre, 2018) ou la *désinformation/mésinformation* (Commission européenne, 2022). Elle a gagné en pertinence publique en raison d'une série d'événements internationaux, tels que ce qui s'est passé avec la Coupe du monde au Qatar (Newtral, 2022), le scandale Cambridge Analytica (Chan, 2020) ou ce qui s'est passé lors des élections présidentielles américaines (BBC World, 2018) ; ce qui a relancé le débat sur ses implications pour les systèmes démocratiques, la perception du public et les intérêts géopolitiques de certains pays. C'est un débat récurrent, où le rôle des réseaux sociaux, des médias traditionnels, des vérificateurs ou de la cybersécurité est souvent mis en avant. Cette réalité polysémique,

confuse et souvent ambiguë rassemble différents concepts qui tentent de nommer, d'expliquer ou de faire allusion à différentes réalités.

2.1. CONCEPTS ET DÉFINITIONS

Désinformation, *fake news* ou post-vérité sont des termes, des mots et des concepts qui sont devenus très populaires, faisant partie du langage familier et souvent utilisés comme synonymes pour tenter de refléter une réalité qui est généralement différente et complexe. Cependant, bien que ces termes soient souvent utilisés de manière interchangeable, chacun d'entre eux possède des nuances et des caractéristiques spécifiques qui les distinguent, ce qui est crucial pour une compréhension plus approfondie du phénomène (DSN, 2022).

Tableau 1

Concept	Définition	Relation avec la vérité
Fake News	Des nouvelles inventées qui ne reposent sur aucun fait	Totalement faux
Post-vérité	Quand les émotions comptent plus que les faits	L'émotionnel prend le pas sur le réel
Désinformation	Informations fausses ou manipulées, délibérément diffusées à des fins stratégiques	Elle mélange des vérités et des faussetés pour produire un effet concret.

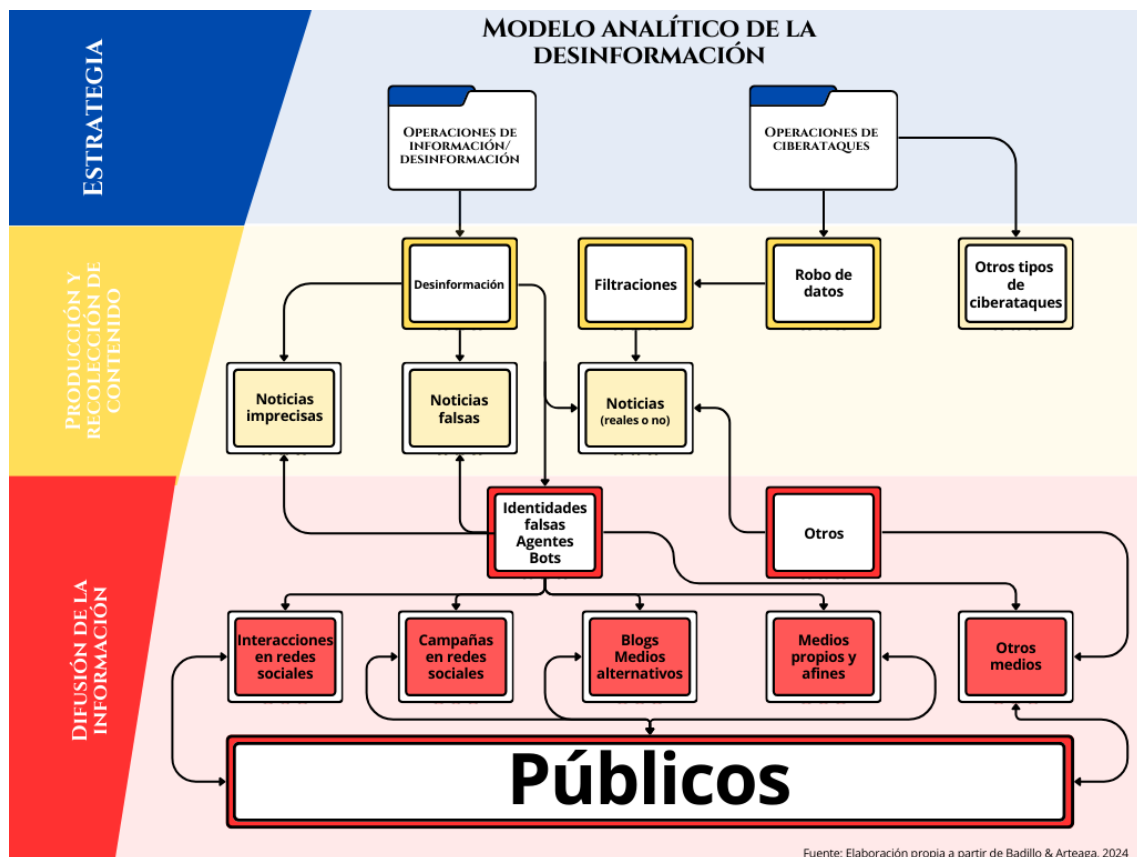
Source : Élaboration propre

Commençons par démêler ce méli-mélo complexe de sujets par l'aspect le plus simple, les *fake news*. Nous entendons par "*fake news*" des informations fausses et fabriquées¹ (Gelfert, 2018). Ces nouvelles sont non seulement fabriquées sans aucun fondement dans la réalité, mais elles sont souvent conçues pour paraître plausibles et manipuler le public, en exploitant les émotions et les préjugés pour maximiser leur impact (DSN, 2022)². Il s'agit de prétendues nouvelles créées à partir de la fantaisie (puisqu'elles n'ont aucun rapport avec la réalité). Sur la base du tableau 1, il est peut-être plus facile de les définir par opposition : il ne s'agit ni de nouvelles réelles mais décontextualisées, ni de nouvelles exagérées (encore une fois, réelles), ni de nouvelles inexactes (avec des éléments réels) (DSN, 2023a). Il est crucial de différencier les "*fake news*" d'autres types de désinformation, comme les nouvelles décontextualisées ou exagérées, car ces dernières, bien que potentiellement trompeuses, sont basées sur des faits réels, ce qui les distingue des nouvelles complètement fabriquées (DSN, 2022). Le modèle analytique de la désinformation proposé par Badillo et Arteaga (2024), présenté dans la figure 1, est particulièrement utile.

¹ Cependant, il ne s'agit pas d'un terme pacifié (Carson, 2018), et bien qu'une évolution vers une différenciation conceptuelle puisse être observée, il existe des auteurs (Flores, 2022) et notamment dans le monde journalistique (IFJ, 2018), où des "arguments" tels que le simple fait que quelque chose soit faux l'invalide pour être une nouvelle (Mayoral, Parratt & Morata, 2019).

² L'utilisation de l'intelligence artificielle a amplifié cette capacité, permettant la création de *deepfakes* et d'autres types de contenus manipulés qui peuvent être diffusés massivement avec une grande rapidité et une grande portée (DSN, 2023a).

Figure 1



La post-vérité³ est un phénomène à multiples facettes (Caridad-Sebastián et al, 2018), où la vraisemblance (Rodrigo Alsina, 2005) est plus pertinente (Rodrigo Alsina, 2005), c'est-à-dire crédible, indépendamment des faits vrais ou réels (Dahlgren, 2018). Dans la post-vérité, les émotions et les croyances personnelles prévalent sur les faits objectifs, ce qui a de profondes implications pour la démocratie et la cohésion sociale, car cela permet à des récits émotifs et souvent trompeurs de prévaloir dans le discours public (DSN, 2022 ; DSN, 2024). Ce phénomène n'altère pas seulement la perception individuelle, mais facilite également la création de "chambres d'écho"⁴ dans lesquelles les gens sont exposés de manière répétée aux mêmes idées, ce qui renforce leurs croyances et les isole d'autres perspectives (DSN, 2023a).

Il existe également de multiples définitions de la désinformation, qui ont évolué au fil du temps et en fonction du secteur ou du domaine dans lequel elles sont utilisées ou esquissées (Arteaga, 2020). Ce terme englobe non seulement la diffusion intentionnelle de fausses informations, mais aussi la manipulation subtile des faits pour déformer la

³ Il n'y a pas de position unique, mais contrairement au concept précédent (et nuancé), il existe un consensus majoritaire sur l'élément central du "vouloir croire" au détriment des faits ou de la réalité (Olmo, 2019). Le phénomène "C'est un mensonge, mais ça pourrait être vrai" <https://twitter.com/hematocritico/status/1241797239779069952?lang=es>

⁴ Une *chambre d'écho* est un phénomène dans lequel les informations, les opinions et les croyances sont renforcées et amplifiées au sein d'un groupe ou d'une communauté fermée, ce qui limite l'exposition à des perspectives différentes (Jamieson et Cappella, 2008). Pour plus d'informations sur les chambres d'écho, voir : *The echo chamber is overstated* (Dubois et Blank, 2018). <https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract>

réalité et confondre le public (DSN, 2022). La DSN, conformément aux postulats de l'UE, le définit comme suit : *"La désinformation est une information fausse ou trompeuse vérifiable qui est créée, présentée et diffusée à des fins lucratives ou pour tromper délibérément le public, et qui est susceptible de causer un préjudice au public"* (DSN, 2022, p. 253).

Bien qu'adéquate, cette définition restreint ou minimise certains des éléments qui figurent dans la stratégie de sécurité nationale⁵, comme la référence au domaine cognitif (DSN, 2021) ou l'accent mis sur l'intentionnalité et les objectifs de ceux qui mènent des campagnes de désinformation (ce qui lui confère un contexte). L'impact cognitif de la désinformation est crucial, car il ne s'agit pas seulement de diffuser de fausses informations, mais aussi d'altérer la perception et le jugement du public, d'éroder la confiance dans les institutions et de favoriser la polarisation sociale (DSN, 2022 ; DSN, 2023a). Cette opinion coïncide avec celle d'autres auteurs comme Artega et Olmo, qui soulignent que *"la désinformation permet de fragmenter, d'isoler et de manipuler des opinions publiques infectées, de discréditer et de remettre en question des faits objectifs et d'accréditer des émotions virtuelles et des perceptions induites comme étant réelles"* (Artega, 2020) et *"lorsque la fausseté devient plus subtile, plus complexe, qu'elle a été créée avec une intentionnalité tactique, qu'elle répond à une stratégie et poursuit des objectifs, c'est alors que l'on peut parler de désinformation"* (Olmo, 2019).

3. STRATÉGIES HYBRIDES ET ZONE GRISE

Les stratégies hybrides sont définies comme une approche du conflit qui combine des éléments conventionnels et non conventionnels, en utilisant une variété d'outils - militaires, économiques, diplomatiques, cybernétiques et d'information - pour atteindre des objectifs stratégiques (Colom, 2018). Ces outils comprennent non seulement la manipulation directe de l'information, mais aussi la création de récits qui modifient la perception du public à long terme, une caractéristique centrale des opérations d'influence et de la désinformation (Torres Soriano, 2022). L'utilisation de ces stratégies se justifie par leur capacité à exploiter les vulnérabilités grâce à une approche qui intègre le domaine militaire à d'autres domaines, tels que le cognitif et l'informationnel, créant ainsi une synergie qui multiplie leur efficacité dans des contextes de faible intensité (Walker, 1998).

La zone grise, quant à elle, se caractérise par l'application de tactiques conçues pour rester en deçà du seuil qui déclencherait une guerre ouverte. Ce concept est fondamental pour comprendre comment les acteurs étatiques et non étatiques défient l'ordre international sans franchir les lignes rouges qui conduiraient à un conflit armé (Martín Renedo, 2022). Dans la pratique, les opérations de la zone grise vont de la coercition économique et de l'utilisation de la désinformation à l'emploi de forces spéciales dans des missions secrètes, conçues pour être difficilement attribuables directement à un État (McCuen 2008). Le chevauchement entre les plans physique, virtuel et cognitif dans la zone grise permet d'exécuter ces stratégies plus efficacement, car la perception du conflit

⁵ Bien que cette définition soit précise, il est important de considérer que la désinformation peut également être motivée par des objectifs non politiques ou non idéologiques, tels que le crime organisé ou la recherche du profit par des acteurs non étatiques (DSN, 2023a ; Marchal González, 2023).

est manipulée pour désorienter les populations cibles et affaiblir leur capacité de réaction (Lupiáñez Lupiáñez, 2023).

Stratégies hybrides⁶ et la "zone grise" est une évolution des tactiques et stratégies historiques de la guerre irrégulière, aujourd'hui renforcée par la technologie moderne et les réseaux d'information, permettant une influence plus efficace et moins détectable dans un contexte mondial (Hafen, 2024). La désinformation, la propagande et les opérations d'influence sont des composantes essentielles de ces stratégies, qui sont déployées dans un environnement de plus en plus complexe et mondialisé (Hoffman, 2009).

La propagande moderne va au-delà de la simple diffusion de messages ; il s'agit d'une manipulation sophistiquée de l'information pour façonner les perceptions et les comportements conformément aux intérêts stratégiques de ceux qui la promeuvent (Calvo Albero, 2017). La propagande⁷ peut être considérée comme une extension des opérations psychologiques, dont l'objectif est non seulement d'influencer l'opinion publique, mais aussi de démoraliser l'adversaire et d'altérer sa capacité de prise de décision (Rid, 2021)⁸. Depuis 2023, ces opérations se sont intensifiées, notamment dans le cadre de conflits mondiaux tels que ceux de l'Ukraine et de Gaza, où la propagande a joué un rôle crucial dans la polarisation de l'opinion publique et la manipulation de l'information à l'échelle internationale (DSN, 2024).

Dans ce contexte, la désinformation n'agit pas seulement comme un outil d'influence, mais facilite également d'autres opérations hybrides en affaiblissant la cohésion sociale et la confiance dans les institutions, créant ainsi un environnement propice à la mise en œuvre de tactiques plus agressives sans qu'il soit nécessaire de recourir à une confrontation militaire ouverte (Alastuey Rivas et al., 2024). Il est essentiel de comprendre que les stratégies hybrides ne sont pas un phénomène nouveau, mais une évolution des tactiques de guerre irrégulière qui ont été employées tout au long de l'histoire, bien que les changements sociaux et les progrès technologiques aient considérablement élargi les outils disponibles pour ces stratégies, permettant leur application à l'échelle mondiale et ayant un impact significatif sur la stabilité internationale (Calvo, 2023). Cela est clairement visible dans la doctrine russe Primakov/Gerasimov, dans la conception chinoise des "trois guerres" ou dans la "nouvelle conceptualisation de la zone grise" occidentale (Adame Hernández, 2024).

3.1. MANIPULATION ET INTERFÉRENCE D'INFORMATIONS ÉTRANGÈRES (FIMI)

Le concept de *manipulation de l'information et d'ingérence étrangère* (FIMI) fait référence à des activités délibérées menées par des acteurs étrangers dans le but de déformer l'information, de manipuler la perception du public et d'influencer les processus politiques et sociaux dans d'autres pays. Selon le rapport conjoint de l'Agence européenne

⁶ Bien que le concept de "guerre hybride" ait fait l'objet de multiples définitions et débats, il n'existe toujours pas de consensus sur sa caractérisation précise, ce qui complique son étude et son application dans l'analyse stratégique contemporaine (Colom, 2018b).

⁷ Plus précisément, la propagande est définie comme un "ensemble de techniques utilisées, de manière systématique, pour diffuser des opinions ou des idées partielles ou biaisées parmi les masses, dans une intention propre, souvent politique" (Donoso Rodríguez, 2020, p. 30), ce qui en fait un outil clé dans les opérations psychologiques.

pour la cybersécurité (ENISA) et du Service européen pour l'action extérieure (SEAE), la FIMI englobe toute une série d'actions, notamment la diffusion de désinformation, la propagande et les opérations psychologiques qui visent à semer la discorde et à déstabiliser les sociétés démocratiques (ENISA & SEAE, 2022). La FIMI peut également impliquer la manipulation de récits culturels et historiques pour attiser les conflits internes et déstabiliser l'ordre social en exploitant des questions sensibles qui résonnent avec les préjugés ou les peurs existant dans une société (Buvarp, 2021). La sophistication de ces opérations réside dans leur capacité à exploiter des fractures préexistantes au sein des sociétés cibles, en exacerbant les divisions et en provoquant des réactions qui sapent la cohésion sociale et politique (Allenby et Garreau, 2017). Ces activités peuvent avoir des conséquences profondes sur la stabilité des institutions démocratiques, car elles s'attachent à exploiter les vulnérabilités sociales et politiques (ENISA & SEAE, 2022).

Dans le contexte de la FIMI, il est essentiel de reconnaître que ces opérations n'impliquent pas toujours la diffusion d'informations totalement fausses. Elles reposent souvent sur des distorsions subtiles de faits réels, en recourant à des techniques telles que la saturation de l'information ou la création de bulles d'information (Rid, 2021), ce qui rend la détection et la réaction difficiles. Ces stratégies, appelées "manipulation subtile de la vérité", sont particulièrement dangereuses car elles jouent avec la perception du public et la crédibilité des sources d'information (Castro Torres, 2021). En outre, la manipulation de l'information par des canaux non traditionnels, tels que les médias sociaux et les plateformes de messagerie instantanée, permet aux acteurs étrangers de maximiser l'impact de leurs campagnes en tirant parti des caractéristiques virales et de la portée mondiale de ces outils (SEAE, 2024).

La FIMI s'inscrit dans le cadre de stratégies hybrides. La propagande et les actions d'influence sont des outils clés dans le cadre de la FIMI. La propagande est utilisée pour promouvoir des récits qui favorisent les intérêts de l'acteur étranger, en utilisant des médias contrôlés ou similaires pour diffuser des messages spécifiques. Ces récits sont soigneusement conçus pour paraître légitimes et s'appuient souvent sur des sources partiales ou biaisées qui donnent de la crédibilité aux messages diffusés (Maggioni et Magri 2015). Ces récits sont conçus pour susciter la méfiance à l'égard des institutions démocratiques et polariser la société (Bennett et Livingston, 2020). En outre, les actions d'influence visent à façonner l'opinion publique ou à influencer les décisions politiques, ce qui peut aller de la manipulation des réseaux sociaux au financement occulte d'acteurs politiques ou médiatiques dans le pays cible (SEAE, 2023). Un exemple récent a été observé lors des élections présidentielles roumaines (Commission européenne, 2024). L'anonymat offert par les plateformes numériques et la possibilité d'opérer par le biais d'intermédiaires ou de *mandataires* ajoutent une couche de complexité au suivi et à l'identification des véritables auteurs de ces campagnes, ce qui rend difficile la mise en œuvre de contre-mesures efficaces (Castro Torres, 2021). L'utilisation de ces méthodes a permis à des acteurs étrangers d'opérer avec une couche supplémentaire d'anonymat et de dénégaration, ce qui complique les efforts pour identifier et contrer ces activités (DSN, 2024).

4. DOMINATION COGNITIVE ET DÉSINFORMATION

Si la conceptualisation du domaine cognitif est relativement moderne, il n'en va pas de même des stratégies qui y sont appliquées, telles que la propagande (Calvo, 2023), l'influence (Jordán, 2018) et la déstabilisation (Quiñones de la Iglesia, 2021). Ces

tactiques ont été historiquement utilisées dans divers contextes géopolitiques, évoluant au fil du temps pour s'adapter aux nouvelles technologies de l'information et aux dynamiques sociales changeantes. Par exemple, la propagande, qui s'appuyait autrefois exclusivement sur les médias traditionnels tels que la presse écrite et la radio, est aujourd'hui diffusée par le biais de plateformes numériques et de médias sociaux, ce qui permet une plus grande pénétration et une plus grande rapidité dans la diffusion des messages. Ces outils ont acquis une sophistication sans précédent, tirant parti de la rapidité et de la portée d'Internet et des réseaux sociaux pour amplifier leurs effets, comme en témoignent les tactiques employées par des groupes tels qu'Al-Qaïda et l'État islamique, qui ont utilisé ces technologies pour influencer l'opinion publique mondiale et légitimer leurs actions (Astorga González, 2020). L'influence des plateformes numériques est telle qu'elles permettent à des acteurs malveillants de segmenter les audiences et de personnaliser les messages, créant ainsi des chambres d'écho qui renforcent les croyances préexistantes et empêchent la diffusion d'informations contraires. Ce phénomène est renforcé par l'utilisation d'algorithmes qui favorisent la polarisation en donnant la priorité aux contenus sensationnalistes et chargés d'émotions, ce qui, à son tour, facilite la manipulation du domaine cognitif à grande échelle (DSN, 2023b).

La théorie structuraliste de la construction idéologique de Louis Althusser, selon laquelle les médias jouent un rôle central dans la création et le maintien des idéologies qui dominent la perception du public, renforce la compréhension de la manière dont les tactiques de désinformation sont intégrées dans le domaine cognitif⁹ (Althusser, 1971). Dans le même ordre d'idées, la manipulation du domaine cognitif implique la création de réalités perçues qui, bien qu'elles ne reflètent pas nécessairement la réalité objective, deviennent la base sur laquelle les décisions politiques et sociales sont prises (Lupiáñez Lupiáñez, 2023). Comme le soulignent divers auteurs tels que Foucault, le langage ne se contente pas de décrire le monde, il agit également sur lui (Foucault, 1972), ce qui renforce l'idée que le domaine cognitif peut être manipulé par la construction de récits qui reconfigurent la réalité perçue.

En ce qui concerne la désinformation, la zone grise se concentrera principalement sur l'établissement du contexte, en utilisant des stratégies telles que la propagande ou la désinformation, dans le but d'acquérir progressivement un avantage stratégique sur l'adversaire, ce qui permettrait d'améliorer l'efficacité des interventions futures (Hernández-García, 2022). Libicki renforce cette idée en expliquant que les opérations cognitives ne cherchent pas toujours à obtenir des résultats immédiats, mais peuvent être conçues pour semer le doute et la confusion, affectant ainsi la capacité de l'adversaire à prendre des décisions efficaces à long terme (Libicki, 2021). Cette approche souligne l'importance du gradualisme dans la stratégie de désinformation, où de petits changements dans la perception et le récit peuvent aboutir à une altération significative de la réalité perçue, faisant perdre à l'adversaire l'initiative et le contrôle de la situation. Dans cette approche, il convient de mettre l'accent sur la concordance entre les objectifs, la vision stratégique et le gradualisme.

⁹ La doctrine militaire espagnole souligne la pertinence du STRATCOM (*Communications stratégiques*) en tant que fonction de gestion qui intègre les INFOOPS (*Opérations d'information*) et les PSYOPS (*Opérations psychologiques*), en appliquant des techniques d'ingénierie sociale et de communication stratégique pour façonner l'environnement informationnel et cognitif. Ces capacités permettent aux forces armées d'atteindre des objectifs qui transcendent les moyens conventionnels, en opérant dans un domaine intangible qui imprègne tous les autres domaines (PDC-01, 2018).

La relation entre la manipulation cognitive et le conflit politique peut également être analysée dans une perspective clausewitzienne. Clausewitz affirme que la guerre est un acte politique rationnel où l'on cherche à démoraliser l'adversaire non seulement par un conflit direct, mais aussi en manipulant les passions de la population et la perception de la réalité (Clausewitz, 1976). Grâce à la désinformation, il est possible d'éroder le moral d'une armée ennemie et, plus encore, de sa population, dans le but de persuader ses décideurs politiques de mettre fin à leur attitude belliqueuse, de provoquer une négociation ou d'obtenir des avantages dans une négociation déjà planifiée (Rodríguez Lorenzo et al, 2023).

Un facteur fondamental à prendre en compte, et qui n'est souvent abordé que de manière secondaire, est la relation et l'impact politiques. Cet aspect, bien que crucial, est souvent sous-estimé dans les analyses de la désinformation, qui mettent davantage l'accent sur les aspects techniques ou tactiques, laissant de côté les implications plus larges pour la gouvernance et la stabilité politique. Dans une logique clausewitzienne, "si la guerre est de nature politique, il est clair que la cible principale n'est pas les forces armées de l'ennemi, mais le leadership politique" (Calvo Alberro, 2017).

C'est l'intersection entre la désinformation utilisée dans les stratégies hybrides et de zone grise, et les objectifs poursuivis (en particulier l'affectation politique) où ils sont liés à la société, à l'agenda et à l'opinion publique (Sartori, 2007). Dans ce contexte, la manipulation de l'information et la création de récits alternatifs n'ont pas seulement un impact au niveau de l'État ou de l'armée, mais ont également de profondes répercussions sur le tissu social et culturel. La construction de ces récits, qui utilisent les films et les médias¹⁰ comme outils de manipulation émotionnelle, reste essentielle pour comprendre comment des récits malveillants peuvent diviser et embrouiller la société (Davis, 2005). La capacité de ces stratégies à modifier la perception du public n'est pas seulement due à la sophistication des tactiques employées, mais aussi à la manière dont ces récits s'alignent sur les préoccupations et les craintes existantes dans la société, en les amplifiant et en les réorientant contre des cibles spécifiques (Castro Torres, 2021).

La construction de récits malveillants, qui cherchent à diviser et à confondre la société, devient un outil puissant pour déstabiliser non seulement les gouvernements, mais aussi les communautés et la cohésion sociale dans son ensemble. La nécessité de créer un récit malveillant qui puisse être exploité à son propre avantage (Rodríguez Lorenzo et al, 2023), un récit attrayant qui soutienne la stratégie hybride (Torres, 2022) et la génération inéluctable d'un récit qui sponsorise, couvre, renforce et protège la zone grise (Hernández-García, 2022), donnent un grand rôle aux cadres cognitifs (Goffman, 2006), à la communication persuasive (Candelas, 2023) et à l'opinion publique (Sartori, 2007). Ces éléments, bien que sous-estimés dans de nombreuses analyses, sont fondamentaux pour comprendre comment la désinformation s'insère dans le tissu social et devient une force de changement, érodant la confiance dans les institutions et modifiant la perception de la réalité. Il est essentiel de comprendre la relation entre la manipulation cognitive et le changement social car, comme le décrivent Berger et Luckmann (2003), la construction sociale de la réalité est un processus dynamique (externalisation,

¹⁰ Un exemple très éloquent est l'utilisation de la communication plus traditionnelle (comme le cinéma) et de la communication numérique (vidéos de haute qualité et de haute production diffusées *en ligne*) dans les stratégies de communication d'organisations aussi peu " occidentales " que *Daesh*. Avec l'utilisation, en plus des aspects techniques, de tactiques émotionnelles et l'exploitation de biais cognitifs tels que l'ancrage, elles sont devenues des éléments clés pour façonner la perception du conflit (Astorga González, 2020).

objectivation et internalisation) qui peut être facilement influencé par des acteurs ayant le contrôle des médias (interaction sociale) et des récits (langage).

5. CONSTRUIRE DES RÉCITS ET DES CADRES

Les récits sont des récits structurés qui cherchent à donner un sens aux événements et à façonner la perception du public. Depuis l'Antiquité, la propagande repose sur la construction de récits qui façonnent la perception du public. Il a été décrit comment les "illusions nécessaires" sont créées¹¹ afin que certains groupes de pouvoir puissent maintenir leur influence sur la société (Herman & Chomsky, 1988). Dans le contexte de la désinformation moderne, les récits sont conçus non seulement pour convaincre, mais aussi pour ancrer des croyances difficiles à éradiquer, même lorsqu'elles s'avèrent fausses¹². Flynn, Nyhan et Reifler (2017) identifient que les perceptions politiques erronées ne sont pas de simples défaillances de l'information, mais sont dues à des perceptions erronées (croyances fausses ou infondées entretenues avec confiance et résistance à la correction), à des facteurs individuels (tels que les biais cognitifs ou les identités partisans ou idéologiques) et à la résistance au changement (passive à la vérification des fausses informations ou aux processus de vérification des faits) ; mais aussi aux environnements médiatique et politique (facilitant l'exposition sélective à des sources).

Ces récits, une fois en place, peuvent continuer à exercer un effet durable en raison de l'inertie cognitive et de la résistance au changement des croyances établies (Libicki, 2021 ; Flynn, Nyhan et Reifler, 2017). Les récits faux et très trompeurs ont tendance à prévaloir en raison de leur capacité à exploiter les émotions humaines, telles que la peur et l'indignation morale, ce qui accroît leur impact et leur diffusion dans les réseaux sociaux (Pennycook & Rand, 2021).

Le concept de *cadrage* fait référence aux structures cognitives qui déterminent la manière dont nous interprétons et comprenons les informations. Ces cadres agissent comme des raccourcis mentaux qui organisent l'information et nous permettent d'interpréter les événements en fonction de schémas de signification préalables. La théorie des cadres cognitifs montre comment les structures interprétatives utilisées par la société pour donner un sens aux événements peuvent être manipulées par le biais d'une communication persuasive (Goffman, 2006). La lutte pour le contrôle de ces cadres est devenue un élément central de la lutte contre la désinformation ; le *cadrage* ne cherche pas seulement à combattre les faussetés, mais aussi à établir des cadres alternatifs qui reconfigurent le débat public (Tuñón Navarro, Oleart, & Bouza García, 2019). Dans le contexte des stratégies hybrides, et par extension du domaine cognitif, les cadres sont utilisés pour attirer l'attention du public sur certains aspects de la réalité tout en cachant

¹¹ Dans *Manufacturing Consent : The Political Economy of the Mass Media* (Herman & Chomsky, 1988), l'expression "illusions nécessaires" n'est pas citée dans le texte. Cependant, le concept est développé tout au long du livre. Le concept d'"illusions nécessaires" provient de l'ouvrage ultérieur *Necessary Illusions* (Chomsky, 1992).

¹² Selon des recherches récentes, la sensibilité à la désinformation n'est pas seulement due à l'esprit partisan, mais aussi à un manque de raisonnement prudent et à l'utilisation d'heuristiques, telles que la familiarité avec l'information et la crédibilité de la source (Pennycook et al., 2021).

ou en déformant d'autres aspects¹³. Ce processus permet à certains récits de prévaloir, non pas en raison de leur véracité, mais de la manière dont ils sont présentés et contextualisés. Ce processus est essentiel pour maintenir le contrôle des récits et empêcher que les prémisses fondamentales des actions entreprises dans un conflit ne soient remises en question (Colom, 2018).

Dans la pratique moderne, le *cadrage* est devenu un outil clé non seulement pour façonner l'interprétation des événements, mais aussi pour influencer les émotions du public, en exploitant les biais cognitifs qui entravent la réflexion critique (Astorga González, 2020).

5.1. MISE EN ŒUVRE

La construction de récits et de cadres dans le contexte de la désinformation implique un processus complexe de création de récits et de structures cognitives destinés à influencer la perception du public de manière profonde et durable. Ce processus repose sur une compréhension approfondie de la science du comportement, où les biais cognitifs tels que l'ancrage, la disponibilité et la confirmation sont exploités pour garantir que les récits construits résistent au changement (Astorga González, 2020). La sophistication dans la construction de ces récits utilise la capacité à combiner des faits réels avec des distorsions subtiles, ce qui les rend plus difficiles à discréditer et plus faciles à accepter pour le public (Rid, 2021). Ainsi, les récits, qui exploitent les préjugés cognitifs et émotionnels du public, sont structurés de manière à être simplifiés et émotionnels, ce qui accroît leur efficacité dans la manipulation des médias (Herman & Chomsky, 1988). Ces récits cherchent non seulement à convaincre, mais aussi à établir une perception de la réalité qui résiste à la correction, même lorsque sa fausseté est exposée¹⁴. L'exposition répétée aux fausses nouvelles augmente leur crédibilité perçue, même lorsqu'elles sont initialement plausibles. Cet effet, connu sous le nom d'"illusion de vérité", joue un rôle crucial dans la permanence et l'acceptation des faux récits (Pennycook et al, 2021).

En outre, le *microciblage* ou la segmentation de la population en fonction de ses croyances et de ses valeurs a permis d'adapter les messages à chaque groupe, et la prolifération de médias et de canaux alternatifs (parfois opaques pour la majorité de la population et de l'opinion publique) a amplifié la capacité de ces cadres à influencer la perception du public, augmentant ainsi l'efficacité de la manipulation (Astorga González, 2020). Cette approche personnalisée de la diffusion de la désinformation maximise l'impact sur les différents segments de la société, favorisant la polarisation et renforçant les croyances préexistantes tout en rendant la détection plus difficile (Maggioni et Magri, 2015).

L'impact de ces récits et cadres est tel que, même lorsqu'ils sont discrédités, ils peuvent continuer à influencer l'opinion publique en raison de l'inertie cognitive, un phénomène dans lequel les croyances précédemment établies sont résistantes au

¹³ La recherche suggère que l'interaction entre les réseaux sociaux et la psychologie humaine, en particulier la tendance à utiliser des raccourcis mentaux et à se fier à la familiarité, contribue de manière significative à la diffusion et à la persistance des fausses nouvelles (Pennycook et al, 2021).

¹⁴ Un autre exemple serait la "guerre mémétique", qui utilise des mèmes et d'autres formes de désinformation virale, cherche à créer et à diffuser des récits qui modifient les perceptions et les émotions du public cible, obtenant un impact durable difficile à contrer, en particulier lorsqu'il s'agit de contenus parodiques et de sources civiles (Arias Gil, 2019).

changement (Libicki, 2021). Ce phénomène est particulièrement évident dans la manière dont certains cadres narratifs persistent dans le discours public longtemps après qu'il a été prouvé qu'ils étaient faux, continuant à influencer la perception et l'action sociales (Juurvee et Mattiisen, 2020). Ainsi, la construction de récits et de cadres devient un outil puissant pour façonner la perception du public et maintenir le contrôle sur l'interprétation de la réalité.

5.2. IMPACT DES RÉCITS ET DES CADRES DANS LE DOMAINE COGNITIF

Les récits et les cadres ont un impact profond sur le domaine cognitif, façonnant non seulement la façon dont les événements sont perçus, mais aussi la façon dont ils sont compris et mémorisés. Il a été noté que la création d'un récit malveillant peut être exploitée au profit de ceux qui contrôlent le récit, ce qui confère un grand pouvoir aux cadres cognitifs et à la communication persuasive (Rodríguez Lorenzo et al, 2023 ; Torres, 2022). Ces éléments sont essentiels pour comprendre comment la désinformation s'inscrit dans le tissu social et devient une force de changement, érodant la confiance dans les institutions et modifiant la perception de la réalité. En outre, ces cadres n'influencent pas seulement la perception individuelle, mais aussi la mémoire collective, conditionnant la manière dont les sociétés se souviennent et apprennent des événements historiques, ce qui peut avoir des répercussions à long terme sur la cohésion sociale et la formation des identités nationales (Aznar Fernández-Montesinos, 2021). La propagande et la désinformation n'opèrent pas seulement par le biais de messages directs, mais façonnent également l'environnement cognitif dans lequel ces messages sont interprétés, créant un climat d'incertitude et de méfiance qui facilite la manipulation de l'opinion publique (Lupiáñez Lupiáñez, 2023).

La manipulation cognitive s'est avérée capable d'altérer non seulement la perception immédiate de la réalité, mais aussi de façonner des schémas de pensée et de comportement à long terme (Astorga González, 2020). L'impact de ces récits dans le domaine cognitif est amplifié par l'utilisation des technologies de l'information qui permettent une diffusion rapide et massive, ce qui rend les effets de la désinformation plus durables et difficiles à contrer (Lupiáñez Lupiáñez, 2023).

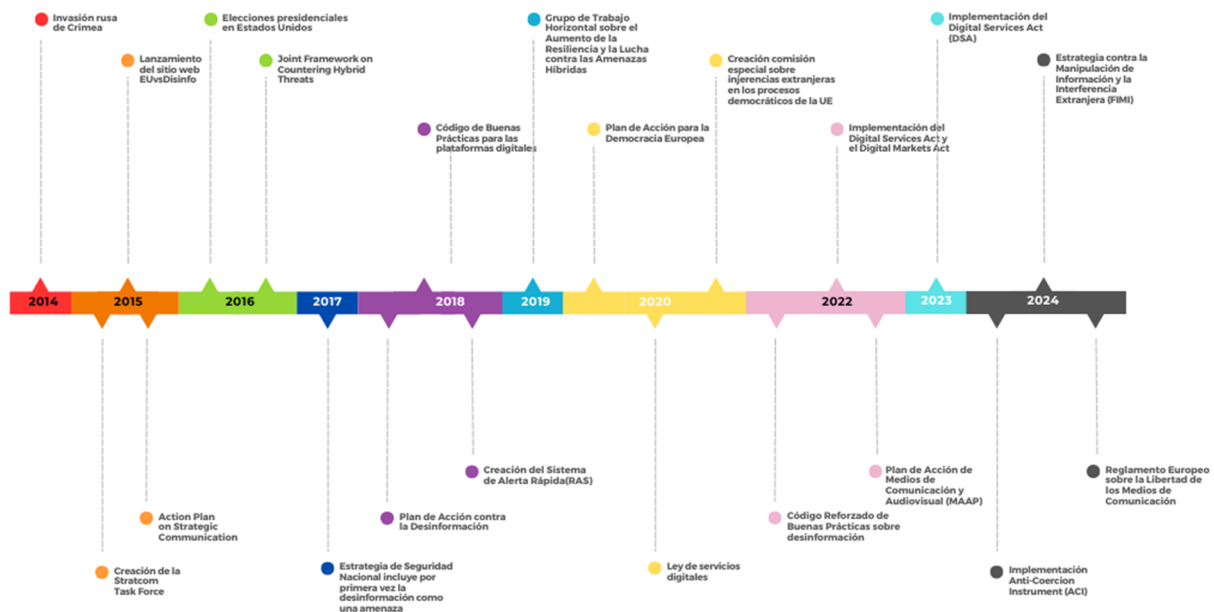
6. ÉVOLUTION DE LA DÉSINFORMATION

L'UE a mis en œuvre un ensemble de politiques et d'actions coordonnées pour lutter contre la désinformation, reconnaissant son impact significatif sur la stabilité démocratique et la sécurité des États membres. La pertinence de cette menace s'est intensifiée après des événements tels que l'invasion russe de la Crimée en 2014 et l'élection présidentielle américaine de 2016, qui ont mis en évidence la manière dont la désinformation pouvait être utilisée comme un outil efficace dans les conflits hybrides et l'ingérence électorale (SEAE, 2015). Les principales étapes sont présentées dans la figure 2.¹⁵

¹⁵ Pour plus d'informations sur l'évolution des actions de l'UE, voir *L'Espagne face à la désinformation : défis hybrides et réponses conventionnelles* (Adame Hernández, 2024).

Figure 2

LAS POLÍTICAS DE LA UNIÓN EUROPEA EN LA LUCHA CONTRA LA DESINFORMACIÓN



Source : Élaboration propre.

En Espagne, la perception de la désinformation a évolué de manière significative au cours des dernières décennies, à partir de la seconde moitié des années 2010, marquée par une reconnaissance croissante des risques associés à la circulation d'informations fausses et manipulées, tant au niveau national qu'international (Badillo et Arteaga, 2024).

La polarisation politique en Espagne, accentuée par le conflit en Catalogne et la fragmentation croissante du spectre politique, a été un facteur important dans la perception de la désinformation (Badillo et Arteaga, 2024). Soixante pour cent des Espagnols perçoivent une grande division politique dans le pays, et plus de 70 % considèrent que la désinformation contribue de manière significative à cette division (CIS, 2021).

La confiance des Espagnols dans les médias reste faible (moins de 5 sur 10)¹⁶, tandis que l'influence des réseaux sociaux augmente¹⁷ (CIS, 2024). L'indice de confiance dans les médias, élaboré par l'Eurobaromètre, révèle un manque de confiance important chez les Espagnols. Quarante pour cent des personnes interrogées en Espagne ne font pas confiance aux médias traditionnels, soit 12 points de plus que la moyenne européenne, et 58 % pensent que les médias fournissent des informations soumises à des pressions

¹⁶ Sur une échelle de 1 à 10 concernant la confiance qu'ils accordent aux médias, celle-ci est passée de 4,3 en 2021 à 4,2 en 2022 et 4,1 en 2023 et 2024. La tendance est d'autant plus prononcée qu'elle diminue avec l'âge : les 25-34 ans l'évaluent à 2,88 et les 18-24 ans à 3,45 (CIS, 2024).

¹⁷ Le pourcentage d'Espagnols influencés par les réseaux sociaux et l'internet lorsqu'ils prennent des décisions politiques est passé de 8,6 % en 2021 à 9,4 % en 2022, 10,3 % en 2023 et 16,2 % en 2024 (CIS, 2024).

politiques ou commerciales, soit 15 points de plus que la moyenne européenne (Eurobaromètre, 2024).

La numérisation et la pénétration des médias sociaux ont joué un rôle crucial dans l'évolution de la perception de la désinformation. Selon l'indice de l'économie et de la société numériques (DESI) 2024, l'Espagne a connu une augmentation constante de l'utilisation de l'internet et des médias sociaux. Le DESI indique qu'en 2024, 96,45 % des ménages espagnols avaient accès à l'internet, 88,23 % de la population avait des compétences numériques supérieures¹⁸ et 34,4 % des entreprises utilisaient plusieurs réseaux sociaux (contre 28,5 % de la moyenne européenne (DESI, 2020)). Ce niveau élevé de connectivité a augmenté l'exposition de la population aux campagnes de désinformation. L'importance croissante des médias sociaux comme principal canal d'accès à l'information¹⁹, en particulier chez les jeunes²⁰, suggère un éloignement des formats d'information traditionnels et une préférence pour les contenus visuels et brefs (Reuters Institute for the Study of Journalism, 2024).

Enfin, le contexte mondial a également influencé la perception de la désinformation en Espagne. La pandémie de COVID-19, par exemple, a déclenché une "infodémie", terme inventé par l'Organisation mondiale de la santé pour décrire la surabondance d'informations, à la fois exactes et inexacts, qui rend difficile la recherche de sources fiables (OMS, 2020). Pendant la pandémie, le réseau Latam Chequea a vérifié plus de 1 000 fausses nouvelles liées au COVID-19 en Espagne, dont beaucoup ont été largement diffusées sur les médias sociaux et les applications de messagerie (Latam Chequea, 2022). Ce phénomène a exacerbé la méfiance du public et déstabilisé davantage l'écosystème de l'information, soulignant la nécessité de renforcer les capacités nationales pour détecter et contrer efficacement la désinformation (OCDE (2024)). Dans un contexte de méfiance croissante à l'égard des médias traditionnels, qui touche près de 70 % de la population (Novoa-Jaso, Sierra, Labiano et Vara-Miguel, 2024). En outre, 37 % des Espagnols évitent activement les nouvelles, un comportement qui semble être motivé par la saturation de contenu négatif ou controversé qui domine les récits médiatiques actuels (Reuters Institute for the Study of Journalism, 2024).

La réponse institutionnelle de l'Espagne à la désinformation a évolué de manière significative depuis 2017, lorsque le problème a été reconnu pour la première fois dans la stratégie de sécurité nationale, jusqu'à la mise en œuvre de politiques plus robustes et coordonnées au cours des années suivantes. Toutefois, cette évolution a été marquée à la

¹⁸ Il s'agit notamment de l'envoi et de la réception de courriers électroniques, des appels téléphoniques ou vidéo sur l'internet, de la messagerie instantanée, de la participation à des réseaux sociaux, de l'expression d'opinions sur des questions civiques ou politiques sur des sites web ou des réseaux sociaux, de la participation à des consultations en ligne ou du vote sur des questions civiques ou politiques.

¹⁹ WhatsApp a dépassé Facebook en tant que principale source d'information en Espagne, 36 % des utilisateurs utilisant WhatsApp pour accéder aux actualités, contre 29 % pour Facebook. Cette transition met en évidence une évolution vers des plateformes plus privées, centrées sur la messagerie (Reuters Institute for the Study of Journalism, 2024).

²⁰ TikTok et Instagram connaissent une croissance rapide chez les moins de 25 ans. TikTok est utilisé par 30 % de cette tranche d'âge pour s'informer, tandis qu'Instagram atteint 25 %, dépassant des plateformes plus traditionnelles comme YouTube, qui se situe à 15 % (Reuters Institute for the Study of Journalism, 2024).

fois par des avancées notables et quelques lacunes dans l'intégration d'approches plus holistiques incluant la gestion narrative (Adame Hernández, 2024).²¹

7. MESURES ET OUTILS ACTUELS DE LUTTE CONTRE LA DÉSINFORMATION EN ESPAGNE

Le cœur de l'infrastructure espagnole de lutte contre la désinformation repose sur la Commission permanente contre la désinformation, qui coordonne la réponse opérationnelle aux campagnes de désinformation. Cette commission agit sous la supervision du secrétaire d'État à la communication, qui dirige la politique de communication stratégique du gouvernement. En situation de crise, la Cellule de coordination de la désinformation gère la réponse en veillant à ce que les actions du gouvernement soient rapides et efficaces (ORDEN PCM/1030/2020, 2020).

Le forum contre les campagnes de désinformation dans le domaine de la sécurité nationale a été l'un des principaux piliers de la stratégie espagnole de lutte contre la désinformation. En 2023, sept documents ont été présentés, abordant diverses facettes du problème, des méthodologies de vérification et de prévention (telles que le *prebunking* et la théorie de l'inoculation²²) à l'analyse de la désinformation russe dans le contexte de la guerre en Ukraine (DSN, 2023b). Fin 2024, ils ont présenté la deuxième édition des travaux du Forum, avançant sur des aspects tels que le rôle des médias et des services de communication des institutions publiques et privées, le FIMI, le lien entre désinformation et discours de haine, et des hypothèses de travail sur l'écosystème médiatique espagnol et l'opinion publique par rapport à la désinformation (DSN, 2024b). Le Forum canalise la coopération publique-privée et publique-sociale, en articulant une approche stratégique et multisectorielle. La profondeur de ses analyses, ainsi que ses efforts pour aborder une réalité complexe, sont clairement démontrés dans l'évolution de ses publications respectives.

Ou d'autres initiatives telles que les campagnes de communication positive du ministère des Affaires étrangères, de l'Union européenne et de la Coopération pour combattre la désinformation par des récits vérifiables²³, le développement d'outils technologiques tels que ELISA²⁴ (Étude simplifiée des sources ouvertes) ou le projet DANGER (INCIBE, (2024), le plan d'action pour la démocratie²⁵ (MPJRC, 2024) ou l'arrêté établissant l'élaboration de la stratégie nationale contre les campagnes de

²¹ Pour plus d'informations sur l'évolution des politiques espagnoles contre la désinformation, voir *España frente a la desinformación : Desafíos híbridos y respuestas convencionales* (Adame Hernández, 2024).

²² Le *prebunking* est une technique de communication préventive qui consiste à exposer les gens à une version affaiblie de la désinformation avant qu'ils n'y soient confrontés, afin d'accroître leur résistance et leur capacité critique face à de futures tentatives de manipulation. Cette stratégie est similaire à l'"inoculation" psychologique, qui vise à générer une immunité cognitive contre les faux récits (Maldita.es, 2023 ; Roozenbeek et al., 2022).

²³ Mise en avant des campagnes "Voto exterior", "Tu Consulado", "Viaja Seguro" et information sur la Ley de Memoria Democrática (DSN, 2024, p. 103).

²⁴ ELISA surveille les sites web soupçonnés de favoriser les campagnes de désinformation, ce qui permet une détection précoce et une réponse plus agile de la part des autorités (CCN-CERT, 2019). En 2023, il a augmenté ses capacités, en intégrant des algorithmes d'intelligence artificielle qui lui permettent d'identifier plus précisément les schémas de désinformation (DSN, 2024).

²⁵ Qui prévoit, entre autres, la mise en œuvre du règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias).

désinformation (arrêté PJC/248/2025, 2025). Il convient de noter l'absence d'études, de rapports ou d'analyses sur l'impact des mesures institutionnelles de lutte contre la désinformation.

7.1. PROCÉDURE D'ACTION CONTRE LA DÉSINFORMATION

La procédure d'action contre la désinformation, réglementée par l'ordonnance PCM/1030/2020, a pour objectif fondamental la création d'un cadre coordonné de détection, d'analyse et de réponse à la désinformation en Espagne (ORDONNANCE PCM/1030/2020, 2020), en particulier dans les situations affectant la sécurité nationale. Cette procédure a été approuvée par le Conseil national de sécurité et s'inscrit dans le cadre des stratégies européennes de lutte contre la désinformation, notamment celles définies dans le plan d'action de l'UE contre la désinformation de 2018.

La procédure s'articule autour de quatre axes fondamentaux : la détection, l'analyse, la réaction et l'évaluation, et de quatre niveaux d'activation. Le secrétariat d'État à la communication est chargé de la coordination générale, en étroite collaboration avec d'autres ministères, le Centre de situation du Conseil national de sécurité et le Groupe de travail contre la désinformation. Ce groupe interministériel est chargé de conseiller et de proposer des actions au Conseil national de sécurité, garantissant ainsi une réponse intégrée et cohérente .²⁶

La mise en œuvre de la procédure a suscité une controverse publique et a conduit plusieurs organisations à déposer des recours et des plaintes devant le tribunal contentieux-administratif²⁷. Elle a également été critiquée pour son manque de clarté dans la définition des compétences et des champs d'action des différentes autorités impliquées (Gómez, 2020 ; Garrós Font & Santos Silva, 2021) ou le manque de ressources spécialisées (Badillo & Arteaga, 2024).

La Cour suprême a fixé des limites très claires au travail et à la portée de la "Procédure d'action contre la désinformation" et des organes qu'elle crée en déclarant qu'elle ne crée ni n'accorde de nouvelles compétences et qu'elle ne peut pas affecter les droits fondamentaux (Cour suprême, 2021). Le protocole se limite donc à un plan d'action interne visant à établir des critères de coordination. Il établit également une définition juridique de la désinformation²⁸, ce que la procédure ne fait pas.

²⁶ L'annexe II présente le fonctionnement et le mode d'action de la commission permanente contre la désinformation (ORDER PCM/1030/2020, 2020).

²⁷ Pour plus d'informations sur la procédure d'action contre la désinformation, voir *España frente a la desinformación : Desafíos híbridos y respuestas convencionales* (Adame Hernández, 2024).

²⁸ Selon l'arrêt, la désinformation s'entend comme "des informations vérifiables, fausses ou trompeuses, créées, présentées et diffusées à des fins lucratives ou pour tromper délibérément le public, et qui sont susceptibles de causer un préjudice au public" (Cour suprême, 2021). Cette définition est tirée de la procédure d'action en matière de désinformation (ORDER PCM/1030/2020, 2020), elle-même tirée de la communication COM (2018) de la Commission européenne. La procédure d'action contre la désinformation s'est limitée, dans son point 1. Contexte, à reproduire la définition de la Commission européenne.

8. CONCLUSIONS

Tout au long de cet article, nous avons analysé la manière dont la désinformation s'inscrit dans un contexte plus large de tactiques et de stratégies géopolitiques, en soulignant son rôle dans la FIMI. Ce contexte plus large est enrichi par l'examen de la manière dont les cadres narratifs sont stratégiquement utilisés pour orienter le débat public vers des récits spécifiques qui favorisent les intérêts de ceux qui les construisent, en minimisant ou en déformant les aspects de la réalité qui pourraient contredire ces intérêts (Tuñón Navarro, Oleart, & Bouza García, 2019 ; Astorga González, 2020). Il a été avancé que la désinformation n'agit pas comme un outil isolé, mais fait partie d'un ensemble coordonné d'actions visant à influencer la perception du public, à manipuler le récit et à créer de l'incertitude dans les processus politiques et sociaux (Hoffman, 2009 ; McCuen, 2008).

La désinformation a eu un impact critique sur des événements clés au cours de la dernière décennie, affectant à la fois la stabilité institutionnelle et la cohésion sociale. Des analyses ont révélé que les politiques publiques en Espagne, tout en tentant de répondre à ces menaces, ont été insuffisantes en raison de leur nature fragmentée et essentiellement réactive (Badillo et Arteaga, 2024). Cela a placé les institutions espagnoles dans une position vulnérable face à des campagnes de désinformation de plus en plus sophistiquées, qui ont exploité les faiblesses de la coordination interinstitutionnelle et l'absence d'une approche préventive globale (Bennett et Livingston, 2020).

La réponse institutionnelle à la désinformation a été limitée par le manque d'intégration entre la cybersécurité et la défense cognitive. L'anonymat offert par les plateformes numériques et la possibilité d'opérer par le biais d'intermédiaires ou de "mandataires" ajoutent une couche de complexité qui rend difficile l'identification des véritables auteurs de ces campagnes (Castro Torres, 2021), ce qui favorise la nécessité d'une stratégie plus proactive et tournée vers l'avenir (Arias Gil, 2019). Bien que des efforts importants aient été déployés pour améliorer la surveillance et la réponse à la désinformation, ils ont été fragmentés et manquent de la cohérence nécessaire pour faire face efficacement aux menaces. L'absence de proposition de stratégie nationale de lutte contre les campagnes de désinformation depuis 2022 (DSN, 2022) en est un exemple. L'activation du niveau 1 de la procédure d'action contre la désinformation en est un bon exemple. Le niveau d'activation le plus bas de la procédure implique l'accord d'organismes publics de haut niveau tels que le secrétaire d'État à la communication, la DSN, le CNI et le secrétaire d'État à la transformation numérique et à l'intelligence artificielle, entre autres (ORDEN PCM/1030/2020, 2020). Elle attribue également un rôle essentiellement réactif, ce qui renforce la réponse et la portée institutionnelles limitées.

Autre exemple, la construction de récits et de cadres par des acteurs malveillants s'est avérée être un formidable défi, car ces tactiques non seulement déforment la réalité, mais sapent également la confiance dans les institutions démocratiques (Berger & Luckmann, 2003 ; Candelas, 2023), un élément qui a été peu abordé dans la réponse institutionnelle espagnole, et où les paris tels que l'alphabétisation numérique ou les vérificateurs de faits (DSN, 2021) donnent des résultats très limités. Luckmann, 2003 ; Candelas, 2023), un élément peu abordé dans la réponse institutionnelle espagnole, et où les paris tels que la culture numérique ou les *vérificateurs de faits* (DSN, 2021) donnent des résultats très limités (Pennycook, Bear, Collins, & Rand, 2020 ; Flynn, Nyhan, & Reifler, 2017). En fait, les récits faux et très trompeurs ont tendance à prévaloir en raison de leur capacité à exploiter les émotions humaines, telles que la peur et l'indignation

morale, ce qui accroît leur impact et leur diffusion dans les réseaux sociaux (Pennycook & Rand, 2021).

L'analyse de l'efficacité des stratégies proposées suggère qu'une approche globale combinant des mesures techniques et cognitives est essentielle pour élaborer une réponse efficace à la désinformation. Les stratégies actuelles, bien que nécessaires, n'ont pas réussi à anticiper les menaces émergentes et à y répondre en raison de leur approche réactive (Badillo et Arteaga, 2024) et partielle qui n'aborde pas les éléments clés du problème tels que les récits. Il est manifestement nécessaire d'adopter une position plus proactive et prospective, permettant aux institutions non seulement de répondre aux menaces actuelles, mais aussi d'anticiper et de neutraliser les futures campagnes de désinformation (Libicki, 2021).

L'une des initiatives proposées par les principaux acteurs est la mise en œuvre de technologies avancées, telles que l'intelligence artificielle et l'apprentissage automatique, qui peuvent jouer un rôle crucial dans l'identification précoce des schémas de désinformation (OTAN, 2021 ; INCIBE, 2024 ; DSN, 2024b ; Commission européenne, 2025). Ces technologies permettent d'analyser en temps réel de grands volumes de données, facilitant la détection d'anomalies qui pourraient indiquer la présence de campagnes de désinformation coordonnées (Rodríguez Lorenzo et al., 2023). Toutefois, comme nous l'avons vu tout au long de cet article, pour que ces outils soient efficaces, il est essentiel qu'ils soient intégrés dans un cadre plus large de défense institutionnelle, comprenant à la fois la cybersécurité et la défense cognitive.

Outre les mesures technologiques, la recherche souligne l'importance de renforcer la société et ses institutions, en augmentant leur profondeur et leurs capacités stratégiques. La lutte contre la désinformation exige un investissement accru en ressources économiques, institutionnelles et humaines (Rodríguez Lorenzo et al., 2023), proportionnel à l'ampleur de la menace. L'intégration de la logique de la société hybride dans les propositions stratégiques et tactiques peut accroître leur efficacité et réduire les coûts d'investissement dans la réponse (Arias Gil, 2020). Cette logique permet une meilleure adaptation aux menaces émergentes et une réponse plus efficace. Il est essentiel pour l'Espagne de développer des capacités nationales robustes, d'autant plus que la FIMI implique non seulement des puissances majeures comme la Russie et la Chine, mais aussi une variété d'acteurs (Badillo & Arteaga, 2024), pour lesquels la réponse ne peut pas s'appuyer exclusivement sur des organismes internationaux tels que l'OTAN ou l'UE.

Il est nécessaire de dépasser le paradigme qui se concentre sur la promotion de la pensée critique et de l'éducation aux médias et de s'orienter vers un concept similaire à celui proposé par Arias Gil, celui de "citoyen stratégique" (2020). Cette nouvelle approche implique de transformer la logique de la responsabilité individuelle, passive, atomisée, partielle et à moyen/long terme, en une réponse sociale plus proactive, collective et coordonnée. Plutôt que de s'appuyer uniquement sur la formation individuelle aux compétences critiques, le citoyen stratégique est une ressource collective, proactive, décentralisée (mais coordonnée) qui peut agir rapidement face aux menaces de désinformation. Ce changement d'approche pourrait permettre une réponse plus dynamique et plus efficace, en s'attaquant aux menaces à court terme et en facilitant une plus grande adaptabilité à l'évolution des tactiques des acteurs de la désinformation.

Une recommandation clé est la nécessité d'une formation, de simulations et de manœuvres spécifiques dans le domaine de la désinformation, semblables à celles réalisées dans d'autres domaines de la sécurité et de la défense. Cette proposition est absente de toute la documentation analysée ci-dessus. Ces activités permettraient aux institutions d'être mieux préparées à identifier et à neutraliser les campagnes de désinformation avant qu'elles ne causent des dommages importants. En outre, il est proposé d'adopter une attitude plus proactive (utilisation de la communication stratégique) et prospective, permettant d'identifier les vecteurs d'attaque potentiels et de prendre des mesures préventives pour les minimiser, les neutraliser ou les atténuer avant qu'ils ne deviennent des menaces réelles. Il s'agit notamment d'intégrer la logique asymétrique de la société hybride, où les réponses tactiques et stratégiques peuvent être plus efficaces et moins coûteuses (Arias Gil, 2020).

Enfin, la création de structures plus denses et coordonnées dans la lutte contre la désinformation est présentée comme une mesure essentielle. Il s'agit notamment de former les cadres moyens de l'administration publique, du secteur privé et de la société civile, en particulier dans les domaines liés à la communication, à la prospective et à l'analyse sociopolitique. Cette formation est cruciale pour garantir que tous les secteurs de la société sont alignés et préparés à faire face aux menaces complexes posées par la désinformation (DSN, 2022). En ce sens, la dispute pour le contrôle des cadres narratifs est devenue un élément central de la lutte contre la désinformation, où l'objectif n'est pas seulement de combattre les faussetés, mais aussi d'établir des cadres alternatifs qui reconfigurent le débat public (Tuñón Navarro, Oleart, & Bouza García, 2019). De même, connaître, éliminer, atténuer ou neutraliser ses propres vulnérabilités culturelles, politiques ou sociales est essentiel pour éliminer les vecteurs d'attaque, réduire les vulnérabilités et accroître la résilience.

En conclusion, il est nécessaire de changer radicalement la manière dont l'Espagne traite la désinformation. Il ne suffit pas de mettre en œuvre des mesures techniques ou réactives ; il est essentiel de développer une stratégie globale qui renforce les aspects sociaux, cognitifs et technologiques, en promouvant une défense plus coordonnée, proactive et adaptative contre les menaces de désinformation dans un environnement hybride mondial de plus en plus dynamique et complexe.

9. RÉFÉRENCES BIBLIOGRAPHIQUES

- Adame Hernández, J. F. (2024). España frente a la desinformación : Desafíos híbridos y respuestas convencionales (Mémoire de maîtrise, Centro Universitario de la Guardia Civil).
- Alastuey Rivas, J., García López, M. I., García Vizcaíno, F., Garrido López, A., Mora Moret, F., Pedrazo Majarrez, J. M., & Pérez-Tejada García, S. (2024). La désinformation comme arme de guerre. Document d'opinion de l'IEEE 26/2024. Institut espagnol d'études stratégiques (IEEE). Consulté sur https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEO26_2024_VVA_A_Desinforma (consulté le 06/04/2025).
- Allcott, H. et Gentzkow, M. (2017). Social media and fake news in the 2016 election (Médias sociaux et fausses nouvelles lors des élections de 2016). *Journal of Economic Perspectives*, 31(2), 211-236. <https://doi.org/10.1257/jep.31.2.211>(consulté le 06/04/2025).
- Allenby, B. et Garreau, J. (2017, 3 janvier). La narration armée est le nouvel espace de combat. *Defence One*. Consulté sur <http://bit.ly/3XyiwB2> (consulté le 14/08/2024).
- Althusser, L. (1971). *Idéologie et appareils idéologiques d'État*. Medellín : La Oveja Negra. Consulté sur <https://lobosuelto.com/wp-content/uploads/2018/10/Althusser-L.-Ideolog%C3%ADa-y-aparatos-ideol%C3%B3gicos-de-estado.-Freud-y-Lacan-1970-ed.-Nueva-Visi%C3%B3n-1974.pdf> (consulté le 14/08/2024).
- Arias Gil, E. (2020). Low-cost insurgency : an emerging asymmetric threat (L'insurrection à faible coût : une nouvelle menace asymétrique). Consulté sur <https://canal.uned.es/video/5f6b02325578f274ac7a0632> (consulté le 06/04/2025).
- Arias Gil, E. (2021). The emerging dimension of fake news : Network-centric warfare and memetic warfare (La dimension émergente des fausses nouvelles : guerre réseau-centrique et guerre mémétique). Extrait de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Rapport. Institut pour le développement du renseignement dans le domaine du terrorisme, de la sécurité et de la défense (IDITESDE). <https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> (consulté le 14/08/2024).
- Arteaga, Félix (2020). La lucha contra la desinformación : cambio de modelo. Real Instituto Elcano. <https://www.realinstitutoelcano.org/comentarios/la-lucha-contra-la-desinformacion-cambio-de-modelo> (consulté le 06/04/2025).
- Astorga González, L. (2020). La manipulation cognitive au 21e siècle. *Revista del Instituto Español de Estudios Estratégicos*, 16, 15-44. Consulté sur <https://revista.ieee.es/article/view/2208> (consulté le 06/04/2025).

- Aznar Fernández-Montesinos, F. (2021). La bataille des récits. Extrait de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Rapport. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). <https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> (consulté le 14/08/2024).
- Badillo, Á. M., et Arteaga, F. (2024). L'impact stratégique de la désinformation en Espagne. Rapport Iberifier. Consulté sur <https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estrategico-de-la-desinformacion-en-espana.pdf> (consulté le 06/04/2025).
- BBC World (16 février 2018). Le ministère américain de la Justice accuse 13 ressortissants russes d'ingérence dans l'élection présidentielle de 2016. <https://www.bbc.com/mundo/noticias-internacional-43092239> (consulté le 04/04/2025).
- Bennett, W. L. et Livingston, S. (2020). The disinformation order : Disruptive communication and the decline of democratic institutions. *European Journal of Communication*. Consulté sur <https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/downloads/The%20Disinformation%20Order%3B%20Livingston.pdf> (consulté le 14/08/2024).
- Berger, P. L. et Luckmann, T. (1966). La construction sociale de la réalité. Buenos Aires. Consulté sur <https://redmovimientos.mx/wp-content/uploads/2020/07/La-Construcci%C3%B3n-Social-de-la-Realidad-Berger-y-Luckmann.pdf> (consulté le 06/04/2025).
- Burkhardt, J. M. (2017). Histoire des fake news. *Library Technology Reports*, 53(8), 5-9. <https://journals.ala.org/index.php/ltr/article/view/6497/8631> (consulté le 06/04/2025).
- Buvarp, P. M. H. (2021). L'espace d'influence : développement d'une nouvelle méthode pour conceptualiser la manipulation de l'information étrangère et l'interférence sur les médias sociaux. The Norwegian Defence Research Establishment (FFI). Consulté sur <https://www.ffi.no/en/publications-archive/the-space-of-influence-developing-a-new-method-to-conceptualise-foreign-information-manipulation-and-interference-on-social-media> (consulté le 02/06/2025).
- Calvo Albero, J. L. (18 décembre 2017). Désinformation : de vieilles idées dans de nouveaux formats. *Global Strategy*. <https://global-strategy.org/desinformacion-viejas-ideas-en-nuevos-formatos> (consulté le 06/04/2025).
- Calvo, J. L. (avril 2023). De la guerre silencieuse à la guerre hybride. *Revista Española de Defensa*. <https://www.defensa.gob.es/Galerias/gabinete/red/2023/04/p-54-57-red-404-desinformacion.pdf> (consulté le 06/04/2025).
- Candelas, M. (2023). La propagande dans les conflits géopolitiques : de la guerre psychologique à la guerre au-delà des frontières. *IEEE Opinion Paper* 02/2023.

https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEE002_2023_MIGCAN_Propaganda.pdf (consulté le 06/04/2025).

Caridad-Sebastián, M, Morales-García, A. M., Martínez-Cardama, S, & García López, F (2018). Infomédiation et post-vérité : le rôle des bibliothèques. https://e-archivo.uc3m.es/bitstream/handle/10016/28096/Infomediacion_EPI_2018.pdf?sequence=1&isAllowed=y (consulté le 20/08/2024).

Castro Torres, J. I. (2021). L'environnement de la désinformation et la construction de récits. Extrait de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Rapport. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). <https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf> [URL non disponible] (consulté le 14/08/2024).

CCN-CERT. (2019, 11 novembre). ELISA : Nouvel outil de cybersurveillance de CCN-CERT. Consulté sur https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Noviembre/Noticia-2019-11-11-ELISA-nueva-herramienta-de-cibervigilancia-del-CCN-CERT.html?idioma=es (consulté le 06/04/2025).

Centre de recherche sociologique (CIS) (2021). Barómetro CIS de febrero-julio de 2022. Madrid, Espagne. Consulté sur <https://www.cis.es/documents/d/cis/es3351marpdf> (consulté le 14/08/2024).

Centro de Investigaciones Sociológicas (CIS) (Centre de recherche sociologique) (2023). Étude 3424 : Perception sociale des aspects scientifiques de la manipulation génétique et de la biotechnologie. Consulté sur <https://www.cis.es/es/detalle-ficha-estudio?origen=estudio&codEstudio=3424> (consulté le 14/08/2024).

Centro de Investigaciones Sociológicas (CIS) (Centre de recherche sociologique) (2024). Étude 3486 : Enquête sur les tendances sociales (IV). Consulté sur https://www.cis.es/visor?migrado=false&fichero=cru3486_enlace (consulté le 01/06/2025).

Chan, R. (2020). Le dénonciateur de Cambridge Analytica explique comment l'entreprise a utilisé les données de Facebook pour influencer les élections. <https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10> (consulté le 06/04/2025).

Chomsky, N. (1992). *Necessary illusions*. Extrait de https://resistir.info/livros/chomsky_ilusiones_necesarias.pdf (consulté le 06/04/2025)

Clausewitz, C. von. (1976). De la guerre. Sphère des livres. Consulté sur <https://www.esferalibros.com/wp-content/uploads/2022/09/De-la-guerra-primera.pdf> (consulté le 14/08/2024).

- Colom, G. (2018). Les guerres hybrides. Quand le contexte fait toute la différence. *Army Magazine*. Consulté sur <https://www.ugr.es/~gesi/Guerras-hibridas.pdf> (consulté le 20/08/2024).
- Colom, G. (2018b). La doctrine Gerasimov et la pensée stratégique russe contemporaine. *Revue de l'armée*. Consulté sur <https://www.thiber.org/2019/05/11/la-doctrina-gerasimov-y-el-pensamiento-estrategico-ruso-contemporaneo> (consulté le 06/04/2025).
- Commission européenne (2022). Le code de bonne pratique renforcé sur la désinformation. Consulté sur <https://ec.europa.eu/newsroom/dae/redirection/document/87585> (consulté le 20/08/2024).
- Commission européenne (2024, 17 décembre). La Commission engage une procédure formelle à l'encontre de TikTok pour risques électoraux en vertu de la loi sur les services numériques. Consulté sur https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487 (consulté le 22/03/2025).
- Commission européenne (2025, 15 avril). La Commission investit 140 millions d'euros pour déployer des technologies numériques clés. Consulté sur https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/la-comision-invierte-140-millones-de-euros-para-desplegar-tecnologias-digitales-clave-2025-04-15_es#:~:text=La%20Comisi%C3%B3n%20ha%20lanzado%20cuatro,y%20luchar%20contra%20la%20desinformaci%C3%B3n (consulté le 22/03/2025).
- Dahlgren, P. (2018). *Médias, connaissance et confiance : l'aggravation de la crise épistémique de la démocratie*. *Javnost - The Public*, 25(1-2), 20-27. Consulté sur <https://doi.org/10.1080/13183222.2018.1418819> (consulté le 06/04/2025).
- Davis, G. (2005). L'idéologie du visuel. Dans M. Rampley (Ed.), *Exploring visual culture : Definitions, concepts, contextes* (pp. 163-178). Edinburgh University Press.
- Tableau de bord DESI pour la décennie numérique (2024). Tableau de bord DESI pour la décennie numérique. Commission européenne. Consulté sur <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts> (consulté le 06/04/2025).
- DSN (2021). Stratégie de sécurité nationale. Département de la sécurité intérieure (2021).
- DHS (2022). Département de la sécurité intérieure (2022). Consulté sur <https://www.dsn.gob.es/sites/default/files/documents/LibroDesinfoSN.pdf> (consulté le 14/08/2024).
- DSN (2023a). Forum contre les campagnes de désinformation dans le domaine de la sécurité nationale - Emplois 2023. Consulté sur <https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf> (consulté le 14/08/2024).

- DSN (2023b). Présentation des travaux 2023 : Forum contre les campagnes de désinformation dans le domaine de la sécurité nationale. Consulté sur <https://www.dsn.gob.es/es/actualidad/sala-prensa/presentaci%C3%B3n-trabajos-2023-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito> (consulté le 14/08/2024).
- DHS. Département de la sécurité intérieure (2024). Rapport annuel sur la sécurité nationale 2023. Gouvernement de l'Espagne. Consulté sur https://www.newtral.es/wp-content/uploads/2024/03/IASN2023_0.pdf (consulté le 14/08/2024).
- DHS. Département de la sécurité intérieure (2024b). Travaux du Forum contre les campagnes de désinformation - Initiatives 2024. Consulté sur <https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/trabajos-foro-contra-campanas-desinformacion-iniciativas-2024#:~:text=medios%20de%20comunicaci%C3%B3n.-,Trabajos%20del%20Foro%20contra%20las%20Campa%C3%B1as%20de%20Desinformaci%C3%B3n%20%2D%20Iniciativas%202024,-Accesible> (consulté le 14/08/2024).
- Donoso Rodríguez, D. (2020). *Implications du domaine cognitif dans les opérations militaires*. *IEEE Magazine*, 01/2020. Consulté sur https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf (consulté le 01/06/2025).
- Dubois, E. et Blank, G. (2018). La chambre d'écho est surévaluée : l'effet modérateur de l'intérêt politique et des médias diversifiés. *Information, Communication & Société*. Consulté sur <https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract> (consulté le 06/04/2025).
- SEAE (Service européen pour l'action extérieure) (2024). 2e rapport sur les menaces FIMI - janvier 2024. Consulté sur https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (consulté le 14/08/2024).
- SEAE, Service européen pour l'action extérieure (2015). Lutte contre la désinformation, la manipulation de l'information étrangère et l'ingérence. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (consulté le 14/08/2024).
- ENISA & SEAE. (2022). Manipulation et interférence d'informations étrangères (FIMI) et cybersécurité - paysage des menaces. Extrait de https://www.cde.ual.es/wp-content/uploads/2022/12/EEAS-ENISA-Disinformation_Misinformation.pdf (consulté le 14/08/2024).

- Eurobaromètre (2024). EUROBAROMETRE STANDARD 102 L'opinion publique dans l'Union européenne. Commission européenne. Consulté sur <https://europa.eu/eurobarometer/surveys/detail/3215> (consulté le 14/08/2024).
- FIJ, Fédération internationale des journalistes (2018). Qu'est-ce qu'une fake news ? Un guide pour lutter contre la désinformation à l'ère de la post-vérité. Consulté sur https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf (consulté le 06/04/2025).
- Flores, J. M. (2022). "Les fake news ont toujours existé, mais aujourd'hui elles ont été catapultées par les réseaux sociaux". Consulté sur <https://www.ucm.es/otri/noticias-las-fake-news-siempre-han-existido-pero-hoy-en-dia-se-han-visto-catapultadas-por-las-redes-sociales> (consulté le 20/08/2024).
- Flynn, D., Nyhan, B. et Reifler, J. (2017). La nature et les origines des perceptions erronées : comprendre les croyances fausses et infondées sur la politique. *Political Psychology*, 38(6), 1053-1077. <https://doi.org/10.1111/pops.12394> (consulté le 06/04/2025).
- Foucault, M. (1972). *L'archéologie du savoir*. Siglo XXI Editores. Tiré de https://monoskop.org/images/b/b2/Foucault_Michel_La_arqueologia_del_saber.pdf (consulté le 14/08/2024).
- Garrós Font, I. et Santos Silva, M. F. (2021). La lutte contre l'infodémie : analyse de la procédure d'action contre la désinformation. *Journal of Communication and Health*, 11(2), 75-89. [https://doi.org/10.35669/rcys.2021.11\(2\).75-89](https://doi.org/10.35669/rcys.2021.11(2).75-89)
- Gelfert, Axel (2018). Fake News : une définition. *Informal Logic*, 38. Consulté sur https://informallogic.ca/index.php/informal_logic/article/view/5068 (consulté le 06/04/2025).
- Goffman, E. (2006). *Analyse des cadres : les cadres de l'expérience*. Centre de recherche sociologique.
- Gómez, A. (2020, 19 novembre). La nouvelle procédure d'action contre la désinformation : La controverse est servie. Blog de Propiedad Intelectual y NNTT Garrigues. Consulté sur <https://blogip.garrigues.com/publicidad/el-nuevo-procedimiento-de-actuacion-contra-la-desinformacion-la-polemica-esta-servida> (consulté le 06/04/2025).
- Hafen, R. (2024). L'art opérationnel chinois : la primauté de la dimension humaine. *Revue militaire*. Consulté sur <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Q2-2024/Hafen-SPA-Q2-2024/Hafen-SPA-Q2-2024-UA.pdf> (consulté le 14/08/2024).
- Herman, E. S., et Chomsky, N. (1988). Les gardiens de la liberté. Extrait de <https://www.labiblioteca.mx/llyfrgell/1783.pdf> (consulté le 06/04/2025).

- Hernández-García, L. A. (2022). La zone grise : une approche conceptuelle du FAS. Consulté sur <https://www.atalayar.com/opinion/luis-hernandez-garcia-ieee/la-zona-gris-una-aproximacion-conceptual-desde-las-fas/20220412121331136376.html> (consulté le 06/04/2025).
- Hoffman, F. (2009). Guerre hybride et défis. *Small Wars Journal*. Consulté sur <https://smallwarsjournal.com/documents/jfqhoffman.pdf> (consulté le 06/04/2025).
- INCIBE (2024). DANGER : Cybersécurité pour la détection, l'analyse et le filtrage de contenus faux ou malveillants dans les environnements hyperconnectés. Extrait de <https://www.incibe.es/node/521663> (consulté le 06/04/2025).
- Jamieson, K. H. et Cappella, J. N. (2008). *Echo chamber : Rush Limbaugh and the conservative media establishment*. Oxford University Press.
- Jordán, J. (2018). Les conflits internationaux dans la zone grise : une proposition théorique dans la perspective du réalisme offensif. *Revista Española de Ciencia Política*, n° 48, consulté sur <https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf>.
(consulté le 20/08/2024).
- Juurvee, I. et Mattiisen, M. (août 2020). La crise du soldat de bronze de 2007 : révision d'un cas précoce de conflit hybride. Centre international de défense et de sécurité. Consulté sur <https://bit.ly/3iRyeZe> (consulté le 06/04/2025).
- Latam Chequea (2022). Fake news about COVID-19 verified by Latam Chequea network (Fausses nouvelles sur COVID-19 vérifiées par le réseau Latam Chequea). Extrait de <https://chequeado.com/investigaciones/como-la-desinformacion-sobre-covid-19-infecto-a-america-latina> (consulté le 14/08/2024).
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Rothschild, D. (2018). La science des fausses nouvelles : un programme de recherche. *Science*, 359(6380), 1094-1096. Consulté sur <https://doi.org/10.1126/science.aao2998> (consulté le 14/08/2024).
- Libicki, M. C. (2021). *Cyberspace in Peace and War*. Naval Institute Press. Consulté sur https://www.researchgate.net/publication/343399173_Military_Operations_in_Cyberspace (consulté le 06/04/2025).
- Lupiáñez Lupiáñez, M. (2023). How to deal with a cognitive attack : Prototype detection of propaganda and manipulation in psychological operations targeting civilians during a conflict (Comment faire face à une attaque cognitive : détection prototype de la propagande et de la manipulation dans les opérations psychologiques ciblant les civils pendant un conflit). *Revista del Instituto Español de Estudios Estratégicos*, (22), 61-93. Consulté sur <https://revista.ieee.es/article/view/6058> (consulté le 14/08/2024).

- MAEUEC, Ministère des Affaires étrangères, de l'Union européenne et de la Coopération (2021). Stratégie d'action extérieure 2021-2024. Consulté sur <https://www.exteriores.gob.es/estrategia2021-2024.pdf> (consulté le 14/08/2024).
- Maggioni, M. et Magri, P. (2018). Twitter et le djihad : la stratégie de communication d'ISIS. *Journal of Cyberspace Studies*, 2(2), 239-241. Consulté sur <https://doi.org/10.22059/jcss.2018.66728> (consulté le 14/08/2024).
- Maldita.es (2023). Qu'est-ce que le prébunking ? Voici comment cette technique permet de lutter contre la désinformation avant qu'elle ne se propage. Extrait de <https://maldita.es/nosotros/20230323/prebunking-que-es-antes-desmentido> (consulté le 06/04/2025).
- Marchal González, A. N. (2023). La nécessité d'un nouveau type de crime : la désinformation en tant que menace pour l'ordre public. *Boletín Criminológico*, 1(2023), 1-14. Consulté sur <https://revistas.uma.es/index.php/boletin-criminologico/article/view/17222/17250> (consulté le 06/04/2025).
- Martín Renedo, S. (2022). Zones grises sur le terrain : la fin des guerres conventionnelles ? IEEE Opinion Paper 93/2022. Consulté sur https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO93_2022_SAU MAR_Zonas.pdf (consulté le 06/04/2025).
- Mayoral, J, Parratt, S, & Morata, M. (2019). Désinformation journalistique, manipulation et crédibilité : une perspective historique. *Histoire et communication sociale*, 24(2), 395-409. Consulté sur <https://revistas.ucm.es/index.php/HICS/article/view/66267> (consulté le 06/04/2025).
- McCuen, J. (2008). Hybrid Wars. *Military Review*, 88(2), 107-113. Consulté sur https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf (consulté le 06/04/2025).
- McIntyre, L. (2018). Posverdad. Madrid : Cátedra.
- MPJRC. Ministère de la Présidence, de la Justice et des Relations avec les Tribunaux (2024). Plan d'action pour la démocratie. Consulté sur https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (consulté le 06/04/2025).
- Newtral (2022). Qatar World Cup, a showcase for hoaxes and misinformation (Coupe du monde du Qatar, vitrine des canulars et de la désinformation). Consulté sur <https://www.newtral.es/bulos-mundial-catar/20221203> (consulté le 06/04/2025).
- Novoa-Jaso, M. F., Sierra, A., Labiano, R. et Vara-Miguel, A. (2024). Digital News Report Spain 2024. Qualité journalistique et pluralité : les clés de la confiance dans l'information à l'ère de l'intelligence artificielle (IA). Servicio de Publicaciones de la Universidad de Navarra. Consulté sur

- https://www.unav.edu/documents/98033082/0/DNR_2024.pdf (consulté le 14/08/2024).
- OCDE (2024), *Faits et mensonges : Renforcer la démocratie par l'intégrité de l'information*, OCDE. Éditions, Paris. Consulté sur <https://doi.org/10.1787/06f8ca41-es> (consulté le 14/08/2024).
- Olmo, J. A. (2019). *Désinformation : concept et perspectives*. Real Instituto Elcano. Consulté sur <https://www.realinstitutoelcano.org/analisis/desinformacion-concepto-y-perspectivas> (consulté le 06/04/2025).
- OMS, Organisation mondiale de la santé (2020). *Gérer l'infodémie COVID-19 : Promouvoir des comportements sains et atténuer les effets néfastes de la mésinformation et de la désinformation*. Consulté sur <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation> (consulté le 14/08/2024).
- Ordonnance PCM/1030/2020, du 30 octobre, qui publie la Procédure d'action contre la désinformation approuvée par le Conseil national de sécurité (2020). *Journal officiel de l'État*. Consulté sur <https://www.boe.es/buscar/doc.php?id=BOE-A-2020-13663> (consulté le 14/08/2024).
- Arrêté PJC/248/2025, du 13 mars, portant publication de l'accord du Conseil national de sécurité du 28 janvier 2025, approuvant la procédure d'élaboration de la stratégie nationale contre les campagnes de désinformation (2025). *Journal officiel de l'État*. Extrait de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151
- OTAN (2021, 12 août). *Lutter contre la désinformation : améliorer la résilience numérique de l'Alliance*. Consulté sur <https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html> (consulté le 14/08/2024).
- OTAN, Siège (2024). *Menaces hybrides et guerre hybride : Programme de référence*. Extrait de https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (consulté le 14/08/2024).
- PDC-01. Publication doctrinale conjointe PDC-01 (A) *Doctrine d'emploi des forces armées*. État-major de la défense, 2018. Consulté sur <https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html> (consulté le 14/08/2024).
- Pennycook, G. et Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25(5), 388-402. Consulté sur [https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613\(21\)00051-6](https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(21)00051-6) (consulté le 06/04/2025).
- Pennycook, G., Bear, A., Collins, E. T. et Rand, D. G. (2020). *Lutter contre la désinformation sur les médias sociaux en utilisant des jugements crowdsourcés de la qualité des sources d'information*. *Proceedings of the National Academy of*

Sciences, 117(7), 2775-2785.
<https://www.pnas.org/doi/abs/10.1073/pnas.1806781116> (consulté le 02/06/2025).

Posetti, J. et Matthews, A. (2018). Petit guide de l'histoire des "fake news" et de la désinformation. Centre international pour les journalistes. Consulté sur https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf (consulté le 06/04/2025).

Quiñones de la Iglesia, F. J. (2021). Désinformation et subversion (2.0) : les techniques de la guerre froide réapparaissent dans le domaine de l'information du 21e siècle. Document-cadre de l'IEEE 12/2021. Consulté sur https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM12_2021_FRA QUI_Desinformacion.pdf (consulté le 06/04/2025).

Institut Reuters pour l'étude du journalisme (2024). Rapport sur l'actualité numérique 2024. Université d'Oxford. Consulté sur <https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024> (consulté le 06/04/2025).

Rid, T. (2021). Désinformation et guerre politique. Barcelone : Crítica.

Rodrigo Alsina, M. (2005). La construcción de la noticia. Consulté sur <https://www.um.es/tic/LIBROS%20FCI-I/La%20produccion%20de%20la%20noticia.pdf> (consulté le 20/08/2024).

Rodríguez Lorenzo, E, Morales, R, Crescente, D, Cabello, M. I, & Paz, I. (2023). L'intelligence artificielle dans la guerre hybride comme arme de désinformation. IEEE Opinion Paper. Consulté sur https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO61_2023_EDU ROD_Inteligencia.pdf (consulté le 06/04/2025).

Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S. et Lewandowsky, S. (2022). L'inoculation psychologique améliore la résilience contre la désinformation sur les médias sociaux. *Science Advances*, 8. Consulté sur <https://www.science.org/doi/10.1126/sciadv.abo6254> (consulté le 06/04/2025).

Sartori, G. (2007). Politique. Lógica y métodos en las ciencias sociales. Fondo de Cultura Económica. Consulté sur <https://maestriainap.diputados.gob.mx/documentos/materia1/sem1/02.pdf> (consulté le 06/04/2025).

SEAE. (2023). Lutte contre la désinformation : manipulation de l'information étrangère et interférence (FIMI). Consulté sur https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (consulté le 14/08/2024).

- Tandoc, E. C., Jr, Lim, Z. W., & Ling, R. (2018). Définir les fake news : une typologie des définitions savantes. *Digital Journalism*, 6(2), 137-153. Consulté sur <https://doi.org/10.1080/21670811.2017.1360143> (consulté le 06/04/2025).
- Terán, E. (2019). La désinformation dans l'UE : menace hybride ou phénomène communicationnel ? Évolution de la stratégie de l'UE depuis 2015 <https://www.idee.ceu.es/Portals/0/Desinformaci%C3%B3n%20en%20la%20UE.pdf> (consulté le 06/04/2025).
- Torres, C. M. (2021). Fake news : the influence of post-truth and disinformation in contemporary politics. *Communication and Society*, 18(2), 199-217. Consulté sur <https://revistas.javeriana.edu.co/index.php/comunicacionsociedad/article/view/31487> (consulté le 14/08/2024).
- Torres-Soriano, M. R. (2022). Influence operations vs. disinformation : differences and points of connection. Consulté sur https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEEO64_2022_MANTOR_Operaciones.pdf (consulté le 01/06/2025).
- Cour suprême (2021, 18 octobre). Sentencia STS 1238/2021. Consulté sur <https://vlex.es/vid/877507365> (consulté le 14/08/2024).
- Tuñón Navarro, J., Oleart, Á., & Bouza García, L. (2019). Acteurs européens et désinformation : le différend entre la vérification des faits, les agendas alternatifs et la géopolitique. *Journal de la communication et de la citoyenneté numérique*, 8(1), 223-238. Consulté sur <https://www.redalyc.org/journal/5894/589466348012> (consulté le 06/04/2025).
- Walker, R. G. (1998). *Spec Fi : The United States Marine Corps and Special Operations*. Monterey, Naval Postgraduate School. Consulté sur <https://apps.dtic.mil/sti/pdfs/ADA359694.pdf> (consulté le 14/08/2024).
- Wardle, C. et Derakhshan, H. (2017). Le désordre informationnel : vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques. Conseil de l'Europe. Consulté sur <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-resear/168076277c> (consulté le 14/08/2024).



Article de recherche

L'INTELLIGENCE SOUS LES FEUX DE LA RAMPE : DE LA THÉORIE CLASSIQUE À UNE NOUVELLE APPROCHE DE LA MISE EN ŒUVRE À L'ÈRE NUMÉRIQUE

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

Paula Castro Castañer

Expert en sécurité chez Telefónica S.A.

Doctorant en sciences médico-légales à l'université d'Alcalá

Master en cybersécurité et vie privée de l'Universitat Oberta de Catalunya (UOC)

paula.castroc@edu.uah.es

ORCID : 0009-0008-0315-8387

Reçu le 14/02/2025

Accepté le 16/06/2025

Publié le 27/06/2025

Citation recommandée : Castro P. (2025). L'intelligence sous les feux de la rampe : de la théorie classique à une nouvelle approche de la mise en œuvre à l'ère numérique. *Logos Guardia Civil Magazine*, 3(2), p.p. 71-100.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

DÉDICACEUR

*A mon tuteur, Hilario, pour m'avoir fait
confiance et m'avoir soutenu dans tous mes
projets.*

L'INTELLIGENCE SOUS LES FEUX DE LA RAMPE : DE LA THÉORIE CLASSIQUE À UNE NOUVELLE APPROCHE DE LA MISE EN ŒUVRE À L'ÈRE NUMÉRIQUE

Résumé: INTRODUCTION. 1.1. NOTE MÉTHODOLOGIQUE. 2. CONCEPT ET ÉVOLUTION DU RENSEIGNEMENT. 2.1. TYPES DE RENSEIGNEMENT. 2.2. ÉVOLUTION DES APPROCHES ET DES STRATÉGIES DE RENSEIGNEMENT. 3. LE CYCLE DU RENSEIGNEMENT. 4. PROPOSITION D'ACTUALISATION DU CYCLE DU RENSEIGNEMENT À L'ÈRE NUMÉRIQUE : LE MODÈLE IDEM. 4.1. EXEMPLE PRATIQUE DE MISE EN ŒUVRE DU MODÈLE IDEM. 5. CONCLUSIONS 6. 5. CONCLUSIONS 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Cet article traite de l'évolution du renseignement dans le domaine de la défense et de la sécurité, depuis les approches traditionnelles jusqu'à son adaptation à l'ère numérique, en établissant une proposition qui répond à certaines des limites signalées dans la littérature sur le cycle classique du renseignement. À cette fin, des concepts clés sont explorés, tels que la définition du concept de renseignement, les différents types de renseignement et même le cycle de renseignement traditionnel et ses phases. En outre, un examen de l'évolution et des différentes approches qui ont été adoptées au cours de l'histoire dans le domaine du renseignement est présenté. Enfin, il propose un modèle de renseignement, appelé IDEM, avec des phases flexibles et combinant le talent des analystes humains et le traitement automatisé des big data pour assurer un renseignement proactif, adaptatif et de qualité face aux cybermenaces transnationales complexes.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Mots clés : cybermenaces, cyberveille, cycle du renseignement, modèle IDEM, approche en réseau

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red

ABBREVIATIONS

ABI : *Intelligence basée sur les activités*

CCN-CERT : Centre national de cryptologie - Équipe d'*intervention en cas d'urgence informatique*

CESID : Centro Superior de Información de la Defensa (Centre supérieur d'information de la défense)

CIA : *Central Intelligence Agency, Agence centrale de renseignement*

CIFAS : Centre d'intelligence des forces armées

CNI : Centre national de renseignement

COMINT : *Communications Intelligence (renseignements sur les communications)*

COP : *police de proximité, police orientée vers la collectivité*

CTI : *Cyber Threat Intelligence, Cyber Threat Intelligence*

CYBINT : *Cyber-renseignement, cyber-renseignement*

ELINT : *renseignement électronique*

FISINT : *Foreign instrumentation signals intelligence (renseignement d'origine électromagnétique)*

GEOINT : *Geospatial Intelligence, renseignement géospatial*

HUMINT : *Renseignement humain*

IDEM : Enhanced Dynamic Intelligence Enrichment and Enhancement (Enrichissement et amélioration dynamiques de l'intelligence)

IDS : *Intrusion Detection System, Système de détection d'intrusion*

ILP : *Intelligence-Led Policing, Police basée sur le renseignement*

IMINT : *Imagery Intelligence (renseignement par imagerie)*

ISR : *Intelligence Surveillance and Reconnaissance (renseignement, surveillance et reconnaissance), Intelligence, surveillance and reconnaissance (renseignement, surveillance et reconnaissance)*

JISR : *Joint Intelligence Surveillance and Reconnaissance (renseignement, surveillance et reconnaissance conjoints), Joint Intelligence, Surveillance and Reconnaissance (renseignement, surveillance et reconnaissance conjoints)*

MASINT : *Measurement and Signature Intelligence* (renseignements sur les mesures et les signatures)

ML : *Machine Learning*, Apprentissage automatique

NLP : *Natural Language Processing* (traitement du langage naturel)

OSCE : *Organisation pour la sécurité et la coopération en Europe*, Organisation pour la sécurité et la coopération en Europe

OSINT : *Open-Source Intelligence* (renseignement de source ouverte)

SCADA : système de contrôle et d'acquisition de données (*Supervisory Control and Data Acquisition*)

SECED : Service central de documentation

SIEM : *Security Information and Event Management* (gestion des informations et des événements de sécurité)

SIGINT : *Signal Intelligence* (renseignement d'origine électromagnétique)

SOCMINT : *Social Media Intelligence*, Social Media Intelligence

TCPED : *Tâche, Collecte, Traitement, Exploitation, Dissémination*, Approche, Collecte, Traitement, Exploitation, Dissémination

TTP : *menaces, techniques et procédures*

1. INTRODUCTION

Dans un monde où l'intelligence artificielle semble dominer l'attention et les préoccupations du public, où l'intelligence sous toutes ses autres formes est-elle reléguée au second plan ? L'omniprésence de l'intelligence artificielle dans les débats contemporains occulte souvent l'importance d'autres types d'intelligence qui sont fondamentaux pour le progrès et le développement de l'humanité.

L'intelligence humaine, dans ses multiples manifestations, reste un pilier irremplaçable pour la prospérité de la société, encore plus dans les contextes complexes et changeants de cette ère numérique. L'une de ces manifestations est la veille concurrentielle, qui permet d'obtenir des recommandations actionnables en traitant des informations sur l'environnement externe à la recherche d'opportunités ou d'évolutions pouvant impacter la position concurrentielle d'une entreprise ou d'un pays (Lee, 2023). Ou encore l'intelligence prospective qui, sur la base d'informations passées et présentes, ainsi que de spéculations futures, tente de "dessiner" une carte cognitive pour déterminer différentes options et réduire le niveau d'incertitude qui accompagne toute décision (Montero Gómez, 2006).

Il est vrai que la croissance exponentielle de la numérisation, de l'exposition et de la mondialisation entraîne l'apparition et l'évolution de nouvelles formes de renseignement en réponse aux nouvelles technologies et méthodes de collecte de données, donnant naissance à des formes de renseignement telles que le renseignement de source ouverte (OSINT) ou le renseignement géospatial (GEOINT), entre autres. Ces disciplines tirent parti de la grande quantité d'informations disponibles pour fournir une vision globale, intégrée et détaillée de divers phénomènes. Toutefois, le renseignement ne doit pas se limiter à la collecte et à l'analyse de données, mais doit également intégrer des considérations éthiques et évaluer les conséquences potentielles à long terme des décisions.

Aujourd'hui, l'information et la technologie sont essentielles à presque tous les aspects de la vie, et le renseignement joue un rôle crucial, en particulier dans le domaine de la cybersécurité, car la capacité d'anticiper, d'identifier et d'atténuer les menaces est essentielle pour préserver l'intégrité, la confidentialité et la disponibilité des systèmes.

Toutefois, la question se pose de savoir si cette capacité est une réalité dans les agences gouvernementales et privées d'aujourd'hui, si le renseignement est efficace pour anticiper et atténuer les risques croissants dans le cyberspace, et si le cycle du renseignement est à jour pour répondre aux exigences de l'ère numérique. Le présent document vise à effectuer une analyse théorique pour répondre à ces questions et évaluer l'efficacité du renseignement dans le contexte actuel.

1.1. NOTE MÉTHODOLOGIQUE

Pour l'élaboration de ce travail, une analyse narrative de la littérature académique et technique relative au renseignement dans les domaines de la défense et de la sécurité, ainsi que son adaptation à l'environnement numérique, a été réalisée. Cet examen a servi de base pour contextualiser l'évolution du concept, analyser de manière critique le cycle classique du renseignement et fournir la base de la proposition du modèle IDEM.

La recherche a été effectuée dans des bases de données universitaires telles que Scopus, Google Scholar et Dialnet, ainsi que dans des sources institutionnelles nationales et internationales. Des mots-clés en espagnol et en anglais ont été utilisés, tels que "cycle du renseignement", "cyber-renseignement", "cyber-renseignement" ou "cyber-menaces". La priorité a été donnée aux publications récentes (2000-2024) qui proposaient des approches théoriques, des modèles méthodologiques ou des analyses critiques du processus de renseignement. Occasionnellement, en raison de l'absence de littérature de source ouverte, des sites web réputés ou des sites web rédigés par des spécialistes techniques du domaine ont été consultés.

Les documents sans support académique ou institutionnel ont été exclus, de même que les textes qui ne traitaient pas spécifiquement de la dimension structurelle ou processuelle du renseignement. La littérature sélectionnée a été organisée autour de cinq axes thématiques : (1) définition du concept de renseignement, (2) classification des types de renseignement, (3) évolution historique et organisationnelle des services de renseignement, (4) examen critique du cycle traditionnel et (5) propositions contemporaines pour son adaptation à l'ère numérique.

Cette approche méthodologique a permis de détecter les lacunes théoriques pertinentes et de servir de base à l'élaboration d'un modèle actualisé qui intègre à la fois la dimension humaine et les capacités technologiques de l'intelligence d'aujourd'hui.

2. CONCEPT ET ÉVOLUTION DE L'INTELLIGENCE

Le terme "intelligence" est un concept abstrait et complexe à délimiter en raison de la multitude d'approches sous lesquelles il peut être étudié. Cette difficulté répond non seulement à la diversité des domaines qui l'analysent, mais aussi aux défis que pose, dans un même contexte, l'établissement d'une définition unique.

Dans le domaine de la défense et de la sécurité, la plupart des auteurs lient la naissance du renseignement à l'émergence des Etats et des relations interétatiques. Cependant, il n'existe pas de consensus sur la définition du renseignement, en raison notamment des différentes approches adoptées dans la pratique par les différents pays (Andric & Terzic, 2023). Cette disparité entrave à la fois les progrès théoriques de son étude et la compréhension approfondie des différentes dimensions et facteurs qui affectent sa pratique (Payá-Santos, 2023).

Dans ce contexte, l'une des premières classifications fondamentales, la trinité, a été établie par Sherman Kent, qui a défini trois réalités pour ce concept : l'intelligence en tant qu'organisation, en tant que processus et en tant que résultat (Díaz Fernández, 2013).

- **Le renseignement en tant qu'organisation** : il s'agit des services de renseignement qui relèvent principalement de l'administration publique, comme le Centre national de renseignement (CNI) et le Centre de renseignement des forces armées (CIFAS) en Espagne. Les fonctions de ces institutions comprennent l'obtention, l'évaluation, l'interprétation et la diffusion de renseignements pour protéger et promouvoir les intérêts de l'Espagne, tant à l'intérieur qu'à l'extérieur du pays ; la prévention, la détection et la neutralisation des menaces à la constitution, aux droits et libertés, à la souveraineté, à la sécurité de l'État, à la stabilité institutionnelle et au bien-être de la population ; la promotion de la

coopération avec les services de renseignement étrangers et les organisations internationales ; l'interprétation du trafic de signaux stratégiques ; la coordination de l'utilisation des moyens de cryptage ; la garantie de la sécurité des informations classifiées ; et la protection de ses propres installations, informations et ressources (Jefatura del Estado, 2002).

- **Le renseignement en tant que processus** : il comprend toutes les activités, généralement englobées dans ce que l'on appelle le cycle du renseignement (examiné plus en détail dans les sections suivantes), qui sont nécessaires pour répondre aux exigences des dirigeants et qui interprètent un environnement, un contexte ou un problème. Ces activités sont considérées comme un processus cyclique continu et vont de la collecte d'informations auprès de diverses sources à la diffusion des données intéressantes pour les utilisateurs finaux, en passant par l'analyse et le traitement de ces informations (Chainey & Chapman, 2013).
- **Le renseignement en tant que produit** : il s'agit du résultat et/ou de la connaissance obtenus, sous quelque forme que ce soit, à l'issue du cycle de renseignement. Ce produit doit influencer la prise de décision et avoir un impact sur le contexte interprété (Chainey & Chapman, 2013).

Récemment, une quatrième dimension a également été proposée : **l'intelligence en tant que culture**, définie par Navarro comme "l'ensemble des initiatives et des ressources qui favorisent la prise de conscience de sa nécessité et fournissent une compréhension civique de sa réalité" (Payá-Santos, 2023).

Quelle que soit l'interprétation retenue, le renseignement vise à réduire l'incertitude intrinsèque à la condition humaine et la complexité du monde contemporain dans la prise de décision pour prévenir et éviter tout danger ou menace (Jordan, 2015).

Pour ce faire, le renseignement s'appuie sur des connaissances théoriques liées à la politique, à l'économie, aux relations internationales, à la sécurité, à la sociologie, à la technologie, à la psychologie, etc. Il est donc essentiel de présenter des équipes de qualité composées d'experts dans les différents domaines afin d'aborder les problèmes sous des angles multiples et de trouver des solutions plus efficaces grâce à une approche transversale.

L'aspect multidisciplinaire récent du renseignement est une conséquence de l'élargissement du concept de sécurité et de la complexité croissante du contexte sociétal où les menaces asymétriques et la cyberguerre sont de plus en plus courantes.

En revanche, l'une des plus anciennes qualités du renseignement est le secret de ses activités et des informations obtenues. Toutefois, l'utilisation croissante de sources ouvertes (OSINT) modifie cette perspective. En outre, la mondialisation et l'expansion de l'utilisation d'Internet ont également une incidence sur les conflits, qui sont de plus en plus transnationaux et nécessitent une coopération internationale en matière de renseignement. Cependant, la protection des sources, en particulier des sources humaines (HUMINT), reste un principe fondamental, tout comme la nécessité de préserver la discrétion dans le traitement des informations afin d'éviter les contre-mesures, la désinformation ou la violation d'opérations sensibles.

En bref, on pourrait établir que le renseignement englobe le processus, le produit et l'institution qui réalise la collecte, l'évaluation et le traitement de l'information (Knight,

2024) en tant qu'outil de prise de décision, afin d'identifier, d'avertir et de prévenir les risques et les menaces, en réduisant l'incertitude (Francisco & Barrilao, 2019). Pour y parvenir, ces tâches doivent être réalisées de manière intentionnelle, opportune, planifiée, "secrète" et organisée (Andric & Terzic, 2023).

2.1. LES TYPES D'INTELLIGENCE

Il existe plusieurs classifications de l'intelligence, mais l'une des plus courantes est celle qui dépend du support dans lequel l'information est trouvée, établissant les types suivants (Kamiński, 2019) :

- **SIGINT** (*Signal Intelligence*) : il s'agit de renseignements obtenus à partir de l'interception de signaux, quelle que soit la manière dont ils sont transmis. Il existe trois sous-catégories : le renseignement sur les communications (COMINT), le renseignement électronique (ELINT) et le renseignement sur les instruments étrangers (FISINT). Il est particulièrement utile pour surveiller les menaces numériques et les conflits hybrides.
- **MASINT** (*Measurement and Signature Intelligence*) : basé sur la mesure d'attributs physiques, tels que les émissions électromagnétiques, les propriétés chimiques ou les caractéristiques acoustiques. Il est utilisé dans le cadre d'opérations militaires avancées et de détection d'armes afin de caractériser, localiser et identifier des cibles.
- **HUMINT** (*Human Intelligence*) : il s'agit de la plus ancienne méthode de collecte d'informations à partir de sources humaines, que ce soit par le biais d'entretiens, d'observations directes, d'infiltrations ou de collaborations avec des acteurs locaux. Elle est essentielle dans les contextes où les technologies ne peuvent y accéder.
- **GEOINT** (*Geospatial Intelligence*) et **IMINT** (*Imagery Intelligence*) : renseignement géospatial et renseignement d'imagerie. Le premier combine des cartes, des données géographiques et des informations de télédétection, tandis que le second se concentre sur l'analyse visuelle d'images satellites, aériennes ou de drones.
- **OSINT** (*Open-Source Intelligence*) : renseignements dérivés d'informations du domaine public sous forme physique, analogique ou numérique dans différents médias, tels que la radio, la télévision, les journaux, les magazines, Internet, les bases de données commerciales, les vidéos, les graphiques, les dessins, les réseaux sociaux, etc. rapports ouverts ou publics. Leur volume, leur accessibilité et leur utilité ont augmenté de façon exponentielle avec l'internet (Stewart Bertram, 2015).
- **SOCMINT** (*Social Media Intelligence*) : il s'agit parfois d'une sous-catégorie de l'OSINT, axée sur les médias sociaux. Il est utilisé pour surveiller les tendances, détecter les menaces émergentes, analyser les perceptions et suivre des acteurs spécifiques (Mahood, 2015).

Cependant, une autre typologie très répandue est celle de leur objectif : stratégique, tactique et opérationnel (Gruszczak, 2018).

- **Veille stratégique** : elle se concentre sur l'identification des risques, des menaces et des opportunités afin de soutenir la définition des objectifs et la prise

de décision, en tenant compte de l'environnement, des acteurs concernés et des évolutions possibles.

- **Renseignement tactique** : se concentre sur la planification et l'exécution d'opérations spécifiques pour atteindre un objectif de portée limitée, dérivé des objectifs généraux du renseignement stratégique.
- **Renseignement opérationnel** : également appelé renseignement opérationnel dans le domaine militaire, il a pour but de permettre l'organisation et l'exécution d'activités pour remplir une mission spécifique (Jiménez Villalonga, 2018).

La coexistence et la complémentarité de ces catégories permettent de construire une intelligence globale, adaptée aux différents niveaux de décision.

2.2. ÉVOLUTION DES APPROCHES ET DES STRATÉGIES EN MATIÈRE DE RENSEIGNEMENT

De nombreux auteurs affirment que le renseignement est aussi vieux que l'histoire de l'humanité, étant donné que la dissimulation d'informations confidentielles et la découverte de celles de l'adversaire ont toujours été des outils permettant d'atteindre et de conserver le pouvoir. En témoignent des civilisations comme la Chine antique avec la sagesse millénaire du maître Sun Tzu (Navarro Bonilla, 2005) ou la Grèce classique avec les procédures de transmission d'informations secrètes d'Énée le tacticien (Vela Tejada, 1993).

À l'origine, le renseignement était un outil au service du pouvoir politique, avec un objectif éminemment militaire : connaître la force, la localisation et les capacités de l'ennemi afin de faciliter la prise de décision du dirigeant. Cependant, à mesure que les sociétés sont devenues plus complexes, leurs menaces se sont accrues, ce qui a conduit à l'élargissement progressif du renseignement vers des aspects sociaux, économiques ou politiques. Ainsi, les activités de renseignement ont pris un rôle crucial avec la naissance des États et des relations entre eux, dans le but de défendre et de protéger les intérêts nationaux (Andric & Terzic, 2023).

Cependant, ce n'est qu'au milieu du XX^e siècle, notamment après les deux guerres mondiales et la guerre froide, que les puissances mondiales ont commencé à organiser formellement leurs services de renseignement (les États-Unis avec la CIA, le Royaume-Uni avec le MI6 et Israël avec le Mossad).

L'Espagne, bien que moins présente au niveau international dans ce domaine, a également tenté pour la première fois de mettre en place un service de renseignement à cette époque. Le Service central de documentation (SECED) a été créé en 1972 et le Centre supérieur d'information de défense (CESID) en 1977, mais ce n'est qu'en 2002 que l'actuel CNI (Centre national de renseignement, 2023) a été fondé.

À partir de là, la révolution technologique et l'explosion du volume d'informations disponibles ont marqué un changement radical : le renseignement a cessé d'être un domaine fermé et exclusivement centré sur l'État pour devenir une activité transversale et dynamique dont les implications dépassent la sphère politico-militaire. Bien que l'essence du renseignement reste la même, les méthodes, le calendrier et les objectifs ont subi de profondes transformations. L'accès massif aux données par le biais de sources ouvertes, l'accélération des flux d'information et la mondialisation des menaces ont réduit le cycle

de vie de l'information et remis en question le rôle central qu'occupait auparavant le secret (Payá-Santos, 2023).

Ce nouveau contexte a été aggravé par les attentats du 11 septembre, qui ont marqué un tournant, soulignant la nécessité d'identifier et de prévenir les menaces asymétriques et transnationales, brouillant la distinction classique entre renseignement interne et externe, et poussant les institutions policières à adopter des modèles plus analytiques, préventifs et collaboratifs (Knight, 2024).

Avec l'extension progressive du renseignement à d'autres domaines stratégiques, tels que le maintien de l'ordre, qui fonctionnait historiquement avec une logique réactive, les fonctions policières ont commencé à évoluer de manière significative. Son approche classique, axée sur la réponse aux crimes accomplis ou aux demandes de service, a été remise en question à mesure que les changements sociétaux et la complexité croissante de la criminalité exigeaient de nouvelles formes d'intervention (Organisation pour la sécurité et la coopération en Europe, 2017). Par la suite, divers courants philosophiques ont influencé le maintien de l'ordre, tels que (Gkougkoudis et al., 2022) :

- **Community Policing ou Community-oriented policing (COP)** : priorité à la coopération entre les citoyens et les forces de l'ordre, favorisant la confiance et la prévention (Carter & Fox, 2019).
- **Police de résolution des problèmes** : elle vise à identifier et à analyser les problèmes sous-jacents à la criminalité dans une perspective plus large et transversale et à rechercher des solutions structurelles et durables (Organisation pour la sécurité et la coopération en Europe, 2017).
- **Police de tolérance zéro** : réponse stricte aux infractions, même mineures, basée sur les idées développées par deux criminologues américains, James Q. Wilson et George Kelling, qui ont publié en 1982 un article intitulé "Broken Windows" (Grabosky, 1999).

Cependant, au cours des dernières décennies, en raison de la complexité des menaces et des risques, de nombreux universitaires et praticiens ont souligné que l'approche holistique la plus efficace pour lutter contre la mondialisation de la criminalité est l'*Intelligence-Led Policing* (ILP), qui se traduit par une police fondée sur le renseignement. Cette approche est apparue dans les années 1990 au Royaume-Uni comme une stratégie visant à améliorer l'efficacité fiscale des services de police, c'est-à-dire à optimiser l'allocation des ressources, la productivité opérationnelle et la qualité des résultats de l'action policière. Initialement mise en œuvre principalement pour lutter contre la grande criminalité et la criminalité organisée, elle a depuis évolué à l'échelle mondiale pour devenir un modèle proactif, fondé sur l'analyse des données et axé sur la prévention, la réduction et la perturbation de tous les types de criminalité. Aux États-Unis, ce sont les événements du 11 septembre 2001 qui ont finalement motivé son adoption, en concentrant son approche sur des formes plus complexes de criminalité (Summers & Rossmo, 2019).

L'ILP est une philosophie proactive visant à identifier et à prévenir les problèmes criminels à l'aide de données brutes et d'analyses mixtes (quantitatives et qualitatives), mais il ne s'agit pas d'une tactique ponctuelle, mais d'un cadre flexible, adaptatif et durable fondé sur des données objectives (Carter & Fox, 2019). Toutefois, sa mise en œuvre se heurte à des défis en termes de clarté terminologique et d'intégration des données, ainsi

qu'à la nécessité de garantir le respect des droits de l'homme dans la gestion du renseignement.

Parallèlement, le modèle de renseignement fondé sur les activités (ABI) a élargi les capacités d'analyse, en particulier face aux menaces émergentes. Ce modèle, dont les origines remontent à la guerre froide, a été développé en raison de la nécessité de gérer et d'analyser d'énormes volumes de données générées par les technologies modernes, telles que les drones et les médias sociaux, en particulier dans le contexte de la lutte contre le terrorisme. Les méthodes d'analyse traditionnelles se sont révélées inadaptées à ce nouvel environnement, car les analystes passent trop de temps à rechercher des informations et à surveiller des cibles connues, ce qui limite leur capacité à découvrir l'inconnu. L'ABI améliore ce processus en permettant la corrélation en temps réel de données provenant de diverses sources, surmontant ainsi les limites des méthodes traditionnelles de renseignement, de surveillance et de reconnaissance (ISR) (Atwood, 2015).

Une autre approche pertinente est le modèle 3i proposé par Ratcliffe en 2006, qui repose sur trois piliers fondamentaux : "interpréter", "influencer" et "avoir un impact" sur l'environnement criminel. Les analystes doivent interpréter activement l'environnement, influencer les décideurs qui, à leur tour, utilisent ces renseignements pour concevoir des stratégies qui affectent l'environnement criminel (Budhram, 2015). En 2016, il a ajouté un i supplémentaire, celui de l'intention, comme le montre la figure 1, soulignant la nécessité de clarifier et de comprendre les objectifs fixés (Organisation pour la sécurité et la coopération en Europe, 2017).

Chiffre 1

Le modèle des 4 i de Ratcliffe : intention, interprétation, influence et impact

Note : Adapté de *OSCE Guidance on Intelligence-led Policing* (p. 24), par OSCE, 2017, OSCE.



Police fondée sur le renseignement (p. 24), par l'OSCE, 2017, OSCE

En bref, le renseignement est passé d'une activité très secrète et centralisée à un processus transversal, interdisciplinaire, distribué et soutenu par la technologie. Cette évolution justifie le besoin de nouveaux modèles tels que l>IDEM, qui intègrent l'analyse humaine et le traitement automatisé pour faire face aux menaces modernes, en particulier dans le cyberspace. En outre, cette trajectoire nous permet d'observer une convergence croissante entre les logiques de sécurité, de défense et de technologie, positionnant le renseignement comme un élément clé de la souveraineté numérique et de la résilience institutionnelle.

3. LE CYCLE DU RENSEIGNEMENT

Bien que l'on attribue souvent à Sherman Kent la formulation scientifique de la méthode de renseignement, des recherches ultérieures ont montré qu'une méthodologie rigoureuse et un ensemble complet d'opérations (ce que l'on a appelé plus tard le cycle du renseignement) avaient déjà été esquissés, par exemple, pendant la guerre civile espagnole (Navarro Bonilla, 2004).

Le cycle du renseignement regroupe toutes les activités qui permettent de transformer l'information brute en renseignement et, comme son nom l'indique, il est de nature cyclique. Le cycle de renseignement classique comporte quatre phases, mais dans certains pays, des phases différentes ou des sous-phases différenciées sont ajoutées. Par exemple, en Espagne, le CCN-CERT établit six phases pour le cycle du renseignement : orientation et planification ; collecte ; transformation ; analyse et production ; diffusion et, enfin, évaluation (National Cryptologic Centre, 2015).

- La première phase, appelée **orientation et planification**, établit le quoi et le comment, c'est-à-dire les exigences du produit de renseignement à produire et les actions à entreprendre pour l'obtenir. L'objet de l'étude, la portée, les objectifs, le délai et le type de rapport doivent être clairs pour que le travail dans les autres phases soit efficace et aboutisse à une qualité supérieure et conforme aux normes juridiques nationales et internationales (Organisation pour la sécurité et la coopération en Europe, 2017).
- L'étape suivante, la **collecte**, consiste à recueillir des données brutes, par exemple à partir des sources mentionnées ci-dessus (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Ce processus est complexe, car les analystes doivent trouver le juste équilibre entre la collecte de toutes les données nécessaires et suffisantes et la surcharge d'informations redondantes. Pour ce faire, ils doivent être conscients de l'existence, de la pertinence, de l'accessibilité et de la fiabilité des sources sélectionnées, ainsi que des contraintes juridiques et des exigences en matière d'autorisation (Organisation pour la sécurité et la coopération en Europe, 2017). En outre, la validité et l'exactitude des informations doivent être évaluées avant de passer aux autres étapes du cycle du renseignement.
- Dans la phase de **transformation**, les données brutes collectées à l'étape précédente sont converties en ensembles structurés tels que des bases de données, des références bibliographiques, etc. Cette étape consiste à cataloguer, hiérarchiser et référencer les informations collectées.
- La quatrième phase, l'**analyse et la production**, se compose des activités par lesquelles les informations transformées sont intégrées, évaluées, analysées et préparées afin d'obtenir le produit final. Au sein de cette phase, deux sous-phases peuvent être établies : la première consiste à intégrer les données obtenues de différentes sources afin d'établir des hypothèses et d'identifier un modèle de renseignement ; la seconde consiste à interpréter les données, c'est-à-dire à aller au-delà des informations obtenues, en réfutant ou en soutenant les hypothèses préétablies (Organisation pour la sécurité et la coopération en Europe, 2017). Généralement, cette phase aboutit à ce que l'on appelle le *renseignement actionnable*, un produit de renseignement qui répond aux exigences définies dans la phase de pilotage et de planification et donc aux besoins du consommateur. Ce produit peut à son tour être de plusieurs types, tels qu'une analyse de tendance, une évaluation à long terme, un renseignement d'actualité,

un renseignement d'estimation ou d'alerte, etc. (National Cryptologic Centre, 2015).

- Au stade de la **diffusion**, le produit final est livré au consommateur qui l'a demandé et, si nécessaire et légalement admissible, il sera également partagé avec d'autres parties prenantes.
- La dernière phase correspond à l'**évaluation**, qui permet un retour d'information continu sur toutes les phases précédentes du cycle du renseignement et sur les résultats obtenus, ce qui permet d'ajuster et d'affiner à la fois les activités individuelles et le cycle dans son ensemble. Cela est particulièrement utile pour répondre de manière optimale à l'évolution des besoins en matière de renseignement.

Cependant, de nombreux experts remettent en question ce modèle traditionnel de l'intelligence et l'une des critiques formulées est la simplification excessive de ce modèle par rapport à la grande complexité du processus réel d'acquisition de l'intelligence. Robert Clark souligne que ce terme "est devenu un concept théologique : personne ne remet en question sa validité", même s'il ne décrit pas les étapes précises à suivre (Phythian et al., 2013).

En outre, Arthur Hulnick souligne que l'idée selon laquelle les clients des services de renseignement guident les producteurs au début du cycle est erronée, car les clients s'attendent souvent à être alertés par le système de renseignement, de sorte que le processus de collecte est principalement motivé par la nécessité de combler les lacunes en matière de données et non par des orientations politiques (Pothoven et al., 2023).

Par ailleurs, les organismes de collecte de données ne sont pas toujours sollicités ; souvent, les bases de données existantes, alimentées depuis des années, sont consultées directement pour préparer un rapport. Ou encore, de nouvelles données brutes peuvent être demandées aux équipes qui les collectent, mais une nouvelle demande de renseignements n'est généralement pas formulée au niveau du client (Jordán, 2011).

Quant à la phase d'analyse, sa définition au sein du cycle du renseignement n'est pas critiquée en soi, mais il est indiqué que c'est l'étape au cours de laquelle la plupart des erreurs sont commises, non pas en raison d'un manque d'informations, mais plutôt le contraire, en raison d'une surcharge de données qui conduit à ce que des informations pertinentes soient ignorées ou interprétées de manière inadéquate par les analystes (Jordán, 2016). Les analystes doivent être conscients de leurs propres processus mentaux et de leurs erreurs potentielles, en évitant les simplifications cognitives involontaires et, bien sûr, les préjugés. En outre, dans certains cas, comme dans les situations de crise, les données brutes arrivent directement sans passer par cette phase.

Quant à la phase de diffusion, elle n'est parfois pas non plus franchie, car toutes les analyses produites ne parviennent pas aux consommateurs. Beaucoup ne sont pas lues par les destinataires et sont stockées directement dans la base de données interne. Dans d'autres cas, les clients ont souvent déjà pris leurs décisions et ignorent les informations qui ne les soutiennent pas.

De même, en ce qui concerne le cycle du renseignement en général, sa définition en tant que séquence de phases finalement disposées de manière circulaire est critiquée, alors qu'il s'agit d'un processus plus dynamique, où toutes les phases s'alimentent les unes les autres et peuvent avancer et reculer dans n'importe quelle direction au sein du cycle. Elle met également en évidence des problèmes d'organisation, de commandement et de

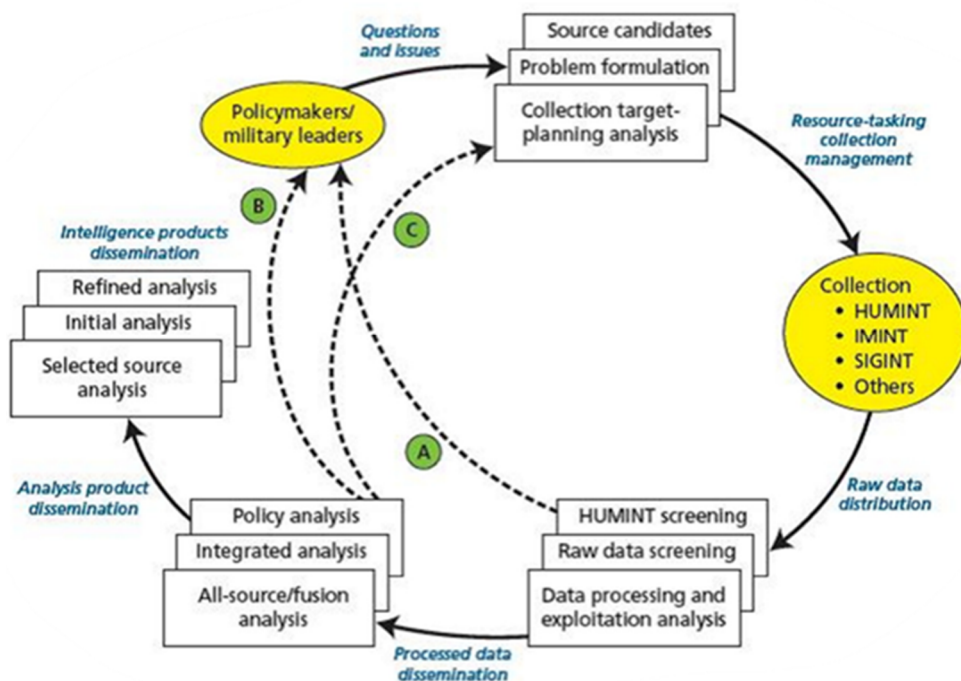
circulation de l'information qui entraînent un manque de flexibilité dans l'action et la communication, ralentissant les processus de prise de décision (Organisation pour la sécurité et la coopération en Europe, 2017).

Des commentateurs tels que Peter Gill et Mark Phythian affirment que le concept de cycle du renseignement a été rendu obsolète par les avancées technologiques, la révolution de l'information et l'évolution des menaces et des cibles. Ils proposent de le remplacer par un "réseau de renseignement" qui reflète mieux les interactions complexes entre le ciblage, la collecte et l'analyse, et met en évidence les facteurs contextuels qui influencent le processus et peuvent être affectés par ses résultats (Pothoven et al., 2023).

D'autre part, plusieurs auteurs ont tenté de saisir la complexité du cycle du renseignement dans des schémas alternatifs au schéma traditionnel. Comme le montre la Figure2, Treverton et Gabbard proposent une approche plus réaliste qui inclut des raccourcis entre les phases, montrant que certaines étapes sont parfois manquées, par exemple que des informations non analysées peuvent parvenir directement aux décideurs. Mark Lowenthal présente un cycle composé de rétroactions constantes, où les nouveaux besoins et les ambiguïtés réactivent le processus, le rendant plus dynamique et multicouche, comme on peut le voir sur Figure3. Robert M. Clark présente le concept de *renseignement centré sur la cible*, un modèle collaboratif et axé sur la cible, dans lequel tous les participants construisent ensemble une image partagée de la question de renseignement qui les intéresse, représentée dans la Chiffre 4 (Jordan, 2016).

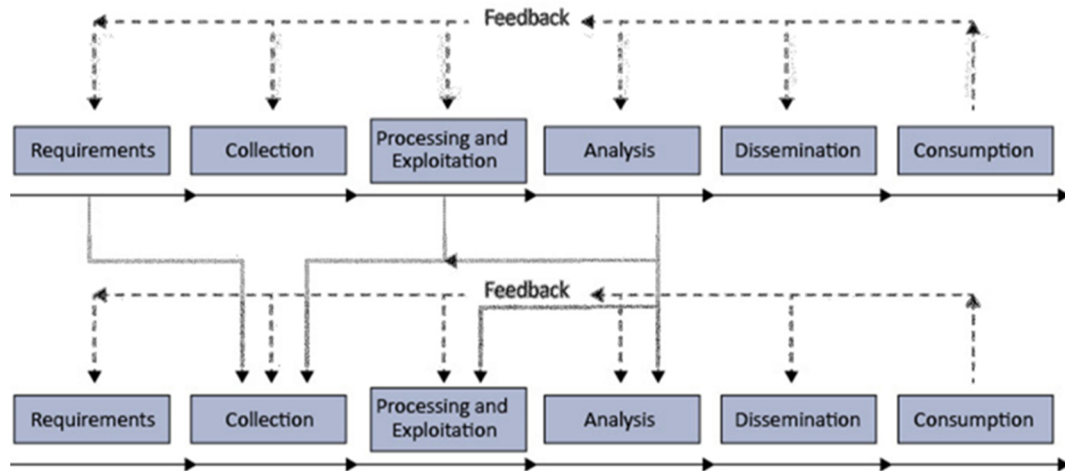
Figure2

L'approche de Treverton et Gabbard



Note : Tiré de *A Review of the Intelligence Cycle* (p. 4) par J. Jordán, 2016, *Analyse GESI (Grupo de Estudios En Seguridad Internacional)*, 2.

Figure3
 Processus multi-strates Mark Lowenthal



Note : Tiré de *A Review of the Intelligence Cycle* (p. 5) par J. Jordán, 2016,
Analyse GESI (Grupo de Estudios En Seguridad Internacional), 2.

Chiffre 4
 Target-Centric Intelligence par Robert M. Clark



Note : Tiré de *A Review of the Intelligence Cycle* (p. 6) par J. Jordán, 2016,
Analyse GESI (Grupo de Estudios En Seguridad Internacional), 2.

Enfin, des propositions telles que le concept JISR (Joint Intelligence, Surveillance and Reconnaissance) de l'OTAN ont également vu le jour. Ce terme désigne l'ensemble intégré de capacités de renseignement et d'opérations qui synchronise et intègre la planification et l'exécution de toutes les capacités de collecte de renseignements, ainsi que leur traitement, leur exploitation et leur diffusion. Ce concept découle de la nécessité d'améliorer le partage des informations et des renseignements pour prévenir les crises, les menaces terroristes, les activités criminelles transnationales et les cybermenaces

(Gruszczak, 2018). Le renseignement, la surveillance et la reconnaissance (ISR) ont toujours été des activités essentielles des opérations militaires, mais elles étaient divisées selon les niveaux de commandement (stratégique, opérationnel et tactique), ou selon les différentes disciplines du renseignement, en fonction du type et de la complexité des sources d'information concernées. Dans le contexte actuel, cette division limite l'utilisation optimale des spécialistes, des agences, des sources et des activités de renseignement. C'est pourquoi le modèle JISR est proposé, dans lequel les activités de renseignement, de surveillance et de reconnaissance fonctionnent comme une seule unité, s'intégrant à tous les niveaux et dans tous les domaines (ministère de la défense, 2023).

Cependant, le modèle JISR présente le même processus que l'ISR, qui se compose de cinq phases : planification, collecte, traitement, exploitation et diffusion (TCPED). La principale différence avec le cycle traditionnel du renseignement est que ce processus n'est ni linéaire ni circulaire, mais que les différentes étapes sont exécutées de manière dynamique, séquentielle, simultanée ou indépendante, en fonction du résultat recherché. Toutefois, dans ce modèle, le processus ISR est généralement aligné sur la phase de collecte du cycle du renseignement, et les résultats de cette collecte sont incorporés dans la phase de traitement, tout en soutenant le cycle de décision.

Toutefois, cette approche est également confrontée à plusieurs limites. Tout d'abord, les ressources peuvent être insuffisantes pour répondre à toutes les exigences, notamment en raison de la forte demande et de la faible disponibilité de certaines capacités de collecte. Il existe également des problèmes techniques tels que les limites de la puissance de calcul et de la bande passante, qui affectent la capacité de traitement et de diffusion des résultats. Les adversaires peuvent interférer par des attaques sur les capacités de RSR, le camouflage, la dissimulation et la désinformation. En outre, l'accès au DSI peut être limité par des obstacles physiques, cognitifs, virtuels, juridiques et politiques (ministère de la défense, 2023).

Aujourd'hui, le renseignement en tant que processus devrait donc s'éloigner des modèles linéaires et cycliques traditionnels pour s'orienter vers des structures plus fluides et en réseau, capables de répondre avec agilité aux menaces émergentes et de tirer parti du vaste volume de données disponibles (Jiménez Villalonga, 2018).

4. PROPOSITION D'ACTUALISATION DU CYCLE DU RENSEIGNEMENT À L'ÈRE NUMÉRIQUE : LE MODÈLE IDEM

Le cycle classique du renseignement a constitué pendant des décennies l'épine dorsale du renseignement en tant que processus. À l'époque, cette représentation séquentielle était logique, car elle facilitait la normalisation, la formation des analystes et la gestion des opérations. Toutefois, le modèle présente des limites importantes lorsqu'il est transposé dans les contextes actuels de complexité, d'incertitude et d'évolution rapide, en particulier dans des domaines tels que le cyberspace.

Dans cet environnement extrêmement dynamique, le renseignement est devenu un outil essentiel pour comprendre et anticiper les menaces, en particulier dans le domaine numérique. À mesure que les organisations étendent leur présence dans le cyberspace pour maximiser leur visibilité et leur portée, elles augmentent également leur exposition à des attaques potentielles. Cette transformation exige de repenser le rôle du

renseignement au-delà de sa formulation classique, en l'adaptant aux particularités d'un environnement décentralisé, interconnecté et en constante évolution.

Toutefois, cette adaptation n'est pas simple. La prolifération des termes et des approches reflète à la fois la jeunesse du domaine et son expansion rapide. Dans certains cadres conceptuels, le terme cyberintelligence ou CYBINT est utilisé comme un sous-type de COMINT (Jiménez Villalonga, 2018), mais il pourrait également être considéré comme un type de renseignement supérieur qui englobe et coordonne les activités OSINT, SIGMINT, SOCMINT et même HUMINT (Portillo, 2019).

Dans le contexte européen, il est plus courant de parler de renseignement sur les cybermenaces (CTI), qui désigne l'application systématique du renseignement pour identifier, analyser et atténuer les menaces qui pèsent sur le cyberspace. Selon Gartner (Lee, 2023), le renseignement sur les cybermenaces repose sur des connaissances factuelles qui fournissent un contexte, des mécanismes, des indicateurs et des conseils pratiques sur les menaces émergentes ou existantes.

C'est pourquoi la CTI joue un rôle crucial en aidant les organisations à développer une stratégie de sécurité proactive qui leur permet de comprendre et d'anticiper les tactiques, techniques et procédures (TTP) des adversaires. Elle facilite également l'identification des menaces à la source et la réponse efficace aux incidents avant qu'ils ne causent des dommages importants.

Cependant, lorsqu'il s'agit de mettre en œuvre des systèmes de recherche ou de travail dans ce domaine, il manque encore des cycles méthodologiques spécifiques et largement acceptés pour structurer le processus de collecte et d'analyse du renseignement cybernétique. Par conséquent, on a tendance à se rabattre sur le cycle traditionnel du renseignement ou sur l'une des approches alternatives existantes. Mais, comme nous l'avons vu, toutes ces approches présentent des limites importantes quant à leur application efficace dans les environnements numériques.

Le **modèle classique** est rigide et séquentiel ; le **modèle proposé par Treverton et Gabbard** permet une certaine flexibilité, mais manque de rétroaction claire ; le **modèle centré sur la cible** propose un cycle continu plus proche de la cible, mais sans structure réellement flexible entre les phases ; et l'**approche multiniveaux de Lowenthal** introduit du dynamisme, mais maintient une certaine linéarité et les connexions bidirectionnelles entre les phases ne sont pas entièrement comprises.

Tableau 1

Tableau comparatif des différents modèles de représentation de l'intelligence en tant que processus

	Modèle classique	Modèle Treverton et Gabbard	Modèle de Mark Lowenthal	Modèle centré sur la cible
Structure	Linéaire ou cyclique (phases successives dans un cercle)	Semi-linéaire (avec des "raccourcis" possibles)	Multi-niveaux (avec des couches actives si nécessaire)	Cyclique (ciblé)
Début du processus	À la demande du consommateur	Semblable à la méthode classique, mais permet de redémarrer à partir de phases intermédiaires.	De nouveaux besoins à la réactivation de phases antérieures	A partir de l'analyse de la cible (à partir d'une analyse précédente ou de nouveaux besoins et informations)
Principales phases	Pilotage et planification, collecte, traitement, analyse et production, diffusion, évaluation	Similaire au modèle classique, mais sans ordre strict ni mention de retour d'information.	Identique à la méthode classique, avec des cycles internes et un <i>retour d'information</i> continu.	Les besoins et les <i>lacunes</i> , la collecte, l'analyse et la diffusion sont étroitement liés à l'objectif suivant
Interaction entre les phases	Limité (retour d'information à la fin)	Moyen (linéaire avec raccourcis)	Décharge (continue et simultanée)	Moyenne (cycles connectés par la cible)
Flexibilité et adaptabilité	Faible (modèle rigide et séquentiel)	Moyen (une certaine fluidité, mais maintien de phases définies)	Élevée (orientée vers une reformulation permanente du processus)	Moyen : (dynamisme autour de la cible)
Diffusion de renseignements	A la fin du processus	Peut être omis ou avancé si le produit l'exige.	Elle peut se produire à différents niveaux et à différents moments, en fonction du cycle interne activé.	Fin du processus, après la phase de production
Retour d'information	A la fin du processus	Pas de référence explicite	À tous les stades	Pas de référence explicite

C'est pourquoi ce travail propose le modèle de renseignement IDEM (Enhanced Dynamic Enriched Intelligence) avec une approche en réseau, non linéaire et hautement adaptative, dans laquelle les phases du processus de renseignement ne se succèdent pas de manière séquentielle, mais interagissent de manière dynamique, flexible et continue, permettant un retour d'information constant entre les phases et les équipes de travail.

Alors que le modèle traditionnel commence par la **direction et la planification**, où les exigences en matière de renseignement sont établies en fonction des besoins du décideur, le modèle IDEM propose de commencer par une phase d'**identification et de hiérarchisation des menaces** en temps réel. L'une des critiques les plus récurrentes du cycle traditionnel est son manque de flexibilité, car une fois les objectifs définis, le processus tend à suivre une trajectoire fixe, ce qui est inefficace dans le contexte actuel, où les menaces évoluent rapidement et ne sont pas toujours alignées sur les besoins précédemment établis. Par conséquent, l'objectif de cette phase devrait être de détecter et de hiérarchiser les menaces émergentes de manière proactive, sans s'appuyer uniquement sur les orientations initiales des consommateurs, qui souvent n'arrivent pas à temps ou ne

sont pas formulées du tout. Cette phase deviendrait un processus dynamique et continu en soi, alimenté par une surveillance constante, une reconnaissance en temps réel des modèles de menaces émergentes et la capacité de réorienter rapidement les efforts de renseignement à mesure que de nouvelles menaces ou des changements de conditions apparaissent (Dahj, 2022).

La phase suivante, la **collecte**, reste fondamentale pour le renseignement en tant que processus, car sans données ni informations, il est impossible d'obtenir des connaissances exploitables. Dans le modèle classique, l'un des plus grands défis consistait à filtrer efficacement de grands volumes de données pour éviter à la fois la saturation de l'information et la perte d'informations critiques. À l'ère numérique, cette tâche est devenue encore plus complexe en raison de l'augmentation exponentielle du nombre de sources et de données disponibles, sous l'effet des nouvelles technologies, de la mondialisation et de la courte durée de conservation de l'information. L'IDEM s'attaque à cette complexité en utilisant des technologies avancées telles que l'*apprentissage* automatique et l'intelligence artificielle, qui permettent une collecte automatisée, continue et complète. Bien qu'ils traitent des volumes nettement plus importants, ces outils permettent de filtrer, de hiérarchiser et d'enrichir les informations en temps réel, garantissant ainsi leur pertinence et leur utilité.

Dans cette approche, il n'est pas utile d'établir une phase spécifique pour la **transformation des données** comme dans le modèle classique. Grâce à des technologies avancées, telles que le traitement du langage naturel (NLP) et les outils d'analyse des *big data*, la conversion des données brutes en informations pertinentes et contextualisées peut se produire simultanément à plusieurs stades du processus. Les données peuvent ainsi être traitées, structurées et analysées en parallèle, ce qui facilite une réponse agile aux nouvelles informations ou aux changements dans l'environnement.

En outre, la séparation entre la **transformation** et l'**analyse** peut entraîner un manque d'intégration et une perte de contexte pendant la transition. C'est pourquoi IDEM remplace ces deux phases du modèle classique par une étape unique de **contextualisation et d'enrichissement** qui se concentre sur la mise en contexte des données, l'interprétation de leur pertinence et la compréhension du lien avec d'autres événements et modèles. De cette manière, l'analyse peut être continuellement mise à jour et ajustée à mesure que de nouvelles données apparaissent et que de nouvelles questions se posent, développant ainsi une capacité d'adaptation continue. Il est également essentiel de traiter et d'intégrer des informations provenant de sources de données multiples, car elles facilitent une interprétation plus approfondie et plus efficace, en particulier dans le contexte actuel de menaces hybrides. Contrairement à l'approche traditionnelle, ainsi qu'aux systèmes ISR classiques, qui établit un processus individuel pour chaque type de source (OSINT, HUMINT, SIGINT, COMINT, etc.) (ministère de la défense, 2023), l'IDEM propose un modèle interconnecté et multi-capteurs, plus efficace dans la détection et l'analyse de phénomènes complexes, comme le suggère la doctrine JISR du ministère américain de la défense, discutée dans la section 2.2

En revanche, le modèle IDEM prévoit une étape spécifique pour la **production de renseignements exploitables**. Alors que, dans le cycle traditionnel, l'analyse et la production se concentrent sur la production de rapports et de recommandations qui aident à la prise de décision, IDEM préconise des produits qui ne sont pas seulement réactifs, mais aussi prédictifs, permettant l'anticipation d'événements et de tendances ou

l'évaluation d'impacts qui facilitent l'ajustement des stratégies et des décisions en temps réel. L'accent est mis ici sur l'intelligence en tant qu'aide à la décision dynamique, et non en tant que produit fermé.

Parallèlement au développement de toutes ces phases, la phase de **retour d'information** définie dans le cycle de renseignement traditionnel est indispensable, mais réinterprétée comme un processus transversal. Pour assurer une amélioration continue et un processus plus efficace, il est crucial que les points d'amélioration ou les faiblesses soient mis en évidence tout au long de chacune des phases. Cela permettra de prendre en compte ces observations non seulement dans les étapes suivantes, mais aussi dans les recherches futures, plutôt que d'attendre l'obtention du produit de renseignement final, comme c'est le cas dans le modèle traditionnel.

Enfin, dans le cycle traditionnel, la **diffusion** est réservée à la fin du processus, une fois que le rapport de renseignement a été produit. IDEM rompt avec cette logique en proposant une diffusion modulaire et progressive, en partageant non seulement le renseignement en tant que tel, mais aussi les menaces reconnues et classées dans la phase d'identification et de hiérarchisation, ou les données collectées à partir des différentes sources disponibles, ou encore les données contextualisées et enrichies dans différents formats. Il est évident que cette diffusion précoce doit être gérée avec soin, en assurant la protection des sources pour éviter les contre-mesures et la désinformation de la part des cibles et pour protéger les sources humaines (HUMINT). Toutefois, la nature transnationale des crimes actuels exige une coopération internationale entre les différents services de renseignement et, par conséquent, un échange d'informations entre eux en temps utile et sans retard pour obtenir des résultats plus efficaces.

Cependant, malgré les capacités techniques offertes par l'automatisation, le rôle de l'analyste humain reste essentiel à chacune des étapes décrites ci-dessus. Les outils automatisés fonctionnent selon des paramètres et des algorithmes définis par leurs programmeurs, qui sont réellement capables d'interpréter les informations dans un contexte plus large, en tenant compte des facteurs culturels, politiques et situationnels. En outre, les modèles prédictifs manquent de flexibilité cognitive pour gérer les ambiguïtés, les contradictions ou les exceptions et peuvent échouer face à des entrées erronées, des données biaisées ou des situations imprévues.

Les analystes, en revanche, sont capables de s'adapter, d'innover et de réajuster leurs approches en réponse à de nouveaux paradigmes, alors que les modèles d'intelligence artificielle ont besoin d'une grande quantité de données d'entraînement pour pouvoir développer de nouvelles méthodologies d'analyse et ne sont pas en mesure d'appliquer des approches créatives si de nouvelles questions se posent. Cette capacité des humains à collaborer au sein des équipes, à discuter des interprétations, à restructurer les stratégies sur la base du *retour d'information* reçu est essentielle à la réussite de la mise en œuvre des stratégies de renseignement (Jordan, 2011).

Tableau 2
Tableau comparatif du modèle classique et du modèle IDEM proposé

	Modèle classique	Modèle IDEM (proposition propre)
Structure	Linéaire ou cyclique (phases successives dans un cercle)	Modulaire, dynamique et en réseau (cercles concentriques et interconnectés)
Début du processus	À la demande du consommateur	Proactive, sans demande préalable
Principales phases	Pilotage et planification, collecte, traitement, analyse et production, diffusion, évaluation	Identification et hiérarchisation, collecte, contextualisation et enrichissement, production de renseignements, retour d'information et diffusion.
Interaction entre les phases	Limité (retour d'information à la fin)	Décharge : phases interactives et bidirectionnelles
Flexibilité et adaptabilité	Faible (modèle rigide et séquentiel)	Très élevé (phases simultanées et réinitialisables)
Diffusion de renseignements	A la fin du processus	transversale et continue dès les premières étapes du processus
Retour d'information	A la fin du processus	Constante : à tous les stades
Technologie appliquée	Non explicitement couvert	Intégration de technologies avancées (IA, ML, NLP, <i>big data</i>)
Participation humaine	Central, mais hiérarchique	Combinaison synergique d'un analyste humain et d'outils automatisés
Applicabilité dans les environnements numériques	Limitée	Élevé (orienté vers les cybermenaces et les scénarios complexes)

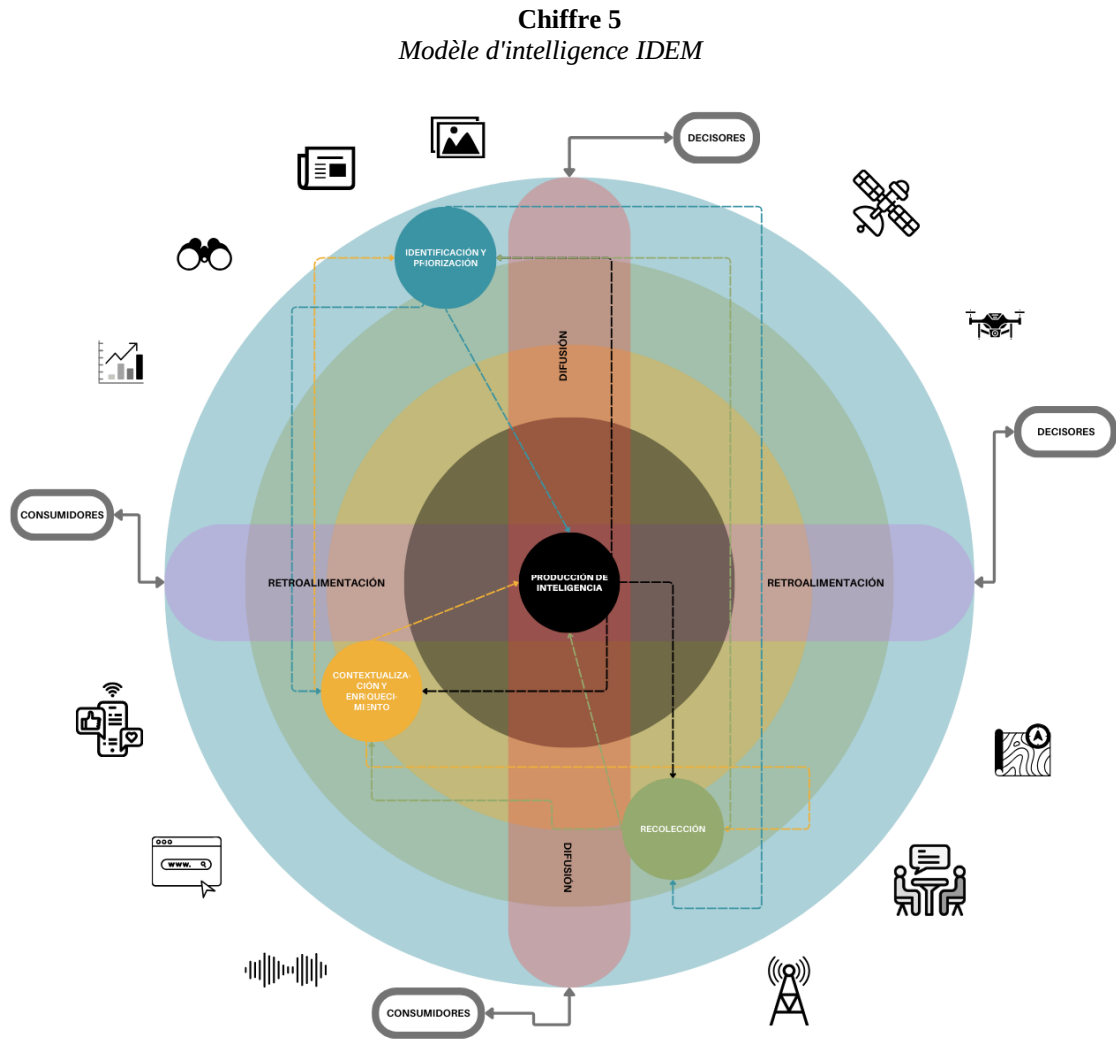
Voici un schéma représentatif du modèle IDEM, dans lequel les différentes phases sont disposées en cercles concentriques. Cette disposition reflète, d'une part, la proximité croissante du produit final de renseignement à mesure que l'on se rapproche du centre et, d'autre part, la nature constante de toutes les étapes, puisque les phases les plus internes sont contenues dans les phases externes. Toutefois, le modèle n'établit pas un parcours linéaire, il n'est pas nécessaire de passer par toutes les étapes pour atteindre le centre. Ce caractère dynamique est représenté par des flèches indiquant les flux possibles d'entrée et de sortie entre les différentes étapes, ce qui permet des transitions directes et bidirectionnelles en fonction des besoins du contexte.

Perpendiculairement à ces cercles et perpendiculairement l'un à l'autre, deux éléments clés sont intégrés, représentés par des rectangles transversaux. Le premier représente la phase de retour d'information, transversale à toutes les phases et opportune pour l'amélioration continue de l'ensemble du cycle. Le second symbolise la phase de diffusion, également collatérale à toutes les étapes et essentielle pour obtenir des produits plus complets et des résultats plus efficaces.

À l'extérieur du schéma se trouvent les consommateurs et les décideurs. Leur nombre et leur importance dépendent à la fois des besoins en matière de renseignement et de l'impact escompté de l'analyse effectuée. Ces personnages sont représentés par des flèches bidirectionnelles, qui indiquent leur double fonction : établir la cible et les critères

du renseignement, tout en recevant des informations en retour ou des produits de renseignement pour faciliter leur prise de décision.

Des icônes provenant de différentes sources d'information sont également incorporées, soutenant ainsi la stratégie de collecte, de contextualisation et d'enrichissement des données provenant de différentes sources pour un processus de renseignement plus complet, plus transversal et plus efficace.



Note : Élaboration propre, Paula Castro Castañer, 2024.

La combinaison de l'adaptabilité, de l'expérience, du jugement critique et du talent humain avec la capacité des machines à traiter de grands volumes de données crée une synergie qui garantit une prise de décision plus efficace, pluridisciplinaire, informée et flexible, tout en assurant une meilleure qualité et pertinence de l'information générée.

4.1. EXEMPLE PRATIQUE DE MISE EN ŒUVRE DU MODÈLE IDEM

Un exemple pratique illustrant l'utilité de l'application de ce modèle de renseignement est celui d'un fournisseur national d'énergie qui détecte une anomalie dans ses systèmes de contrôle SCADA. Dans cette situation, il n'y a pas encore d'incident confirmé ni de demande explicite de la part des décideurs (car ils ne sont probablement pas encore au

courant de cette situation), ce qui implique que l'activation du processus de renseignement se fait de manière proactive et autonome, sur la base de signaux identifiés dans l'environnement opérationnel. Toutefois, l'équipe de renseignement interne active le modèle IDEM afin d'anticiper s'il s'agit d'une menace réelle ou d'une fausse alerte.

L'IDS émet une alerte automatique concernant un trafic anormal vers les serveurs de sauvegarde, ce qui déclenche la phase d'identification et de hiérarchisation. Cette alerte, bien que préliminaire, est suffisante pour que l'équipe de renseignement interne classe la menace comme prioritaire, compte tenu de l'impact potentiel qu'une compromission de cette nature pourrait avoir sur l'infrastructure critique du pays. En conséquence, il est décidé de supprimer temporairement la priorité accordée aux enquêtes ouvertes sur les campagnes d'hacktivisme et à la surveillance géopolitique à faible impact, ainsi qu'à d'autres tâches de surveillance de routine dans les forums et canaux obscurs. Cette réorientation permet de concentrer les efforts humains et technologiques sur une seule hypothèse de travail : une éventuelle intrusion ciblée avancée.

La collecte est déclenchée simultanément à partir de multiples sources internes (journaux, SIEM, enregistrements d'authentification) et externes (flux de renseignements cybernétiques, bases de données d'indicateurs de compromission, alertes émanant d'entités coopérantes ou de fournisseurs de renseignements). Au cours de cette étape, lorsque des indices suggèrent des motivations économiques derrière l'attaque possible, comme, par exemple, l'extraction de données de marché au lieu d'informations opérationnelles, le processus revient brièvement à la phase d'identification afin de reformuler l'hypothèse initiale. Ce retour permet à l'analyse de se concentrer sur la possibilité d'un cas d'espionnage économique industriel en cours de développement, ce qui modifie l'orientation des activités restantes du processus de renseignement.

Dans la phase de contextualisation et d'enrichissement, les données collectées sont intégrées aux informations historiques provenant d'incidents antérieurs et à l'analyse des tendances dans le secteur de l'énergie. Des techniques d'analyse comportementale, d'attribution de TTP et d'exploration de données historiques sont utilisées. Ces méthodologies facilitent la détection de schémas et de coïncidences avec des campagnes précédemment attribuées à des acteurs étatiques ou à des groupes intermédiaires, c'est-à-dire des entités opérant en tant que mandataires ou agents indirects d'autres acteurs ayant des intérêts géopolitiques ou économiques.

Les renseignements sont diffusés sous différents formats adaptés aux besoins spécifiques de chaque type de destinataire. Il peut s'agir d'alertes tactiques destinées aux équipes de cybersécurité chargées d'apporter une réponse immédiate, de rapports stratégiques destinés aux responsables des systèmes énergétiques et de recommandations préventives destinées aux autres opérateurs du secteur afin de renforcer leur position de défense.

Il est important de noter que cette production et cette diffusion de renseignements se font en continu et parallèlement au développement de l'enquête, sans attendre une "conclusion définitive". Cette approche permet une réponse précoce et dynamique aux menaces émergentes, puisque d'autres acteurs concernés du secteur de l'énergie pourraient signaler des incidents similaires dans leurs réseaux après avoir reçu ces produits, ce qui permettrait de rouvrir des cycles d'analyse et de réajuster la hiérarchisation des menaces à l'échelle nationale.

Outre le retour d'information externe de la part des acteurs concernés, qui permet d'ajuster les hypothèses et les priorités en fonction des signaux émis par l'environnement, il existe également une phase continue de retour d'information interne visant à améliorer le processus de renseignement proprement dit. Par exemple, au cours de la phase de contextualisation, l'équipe de renseignement détecte que certains indicateurs clés de compromission (IoC) n'ont pas été considérés comme prioritaires par les systèmes d'alerte automatisés. Cette observation est documentée et transmise à l'équipe chargée d'ajuster les seuils de sensibilité du SIEM, ce qui permet d'affiner les critères de détection pour de futurs cas similaires. Enfin, à la fin du cycle, un examen interne des performances du modèle IDEM dans ce cas précis est effectué, évaluant des paramètres tels que le temps de réponse, la précision des hypothèses initiales et l'utilité des produits générés. Cette évaluation alimente une base de connaissances interne qui permet d'ajuster les méthodologies, les outils et les flux de travail, en veillant à ce que le modèle évolue de manière adaptative et sur la base de l'expérience accumulée.

Cette dynamique de retour en arrière, de reformulation et d'action simultanée permise par le modèle IDEM ne serait pas réalisable dans le modèle classique du cycle du renseignement, ni dans de nombreux modèles proposés dans la littérature examinée, où les processus sont plus rigides, linéaires et dépendent de l'initiative des décideurs.

5. CONCLUSIONS

Le renseignement, entendu comme organisation, processus, produit et même culture, joue un rôle clé dans la gestion de l'incertitude dans des environnements de menaces volatiles, interconnectés et de plus en plus hybrides. Sa nature multidisciplinaire et la diversité des approches utilisées par les différents pays et disciplines rendent difficiles une définition unique et une classification fermée de ses types, mais reflètent également sa richesse conceptuelle et la nécessité d'une coopération et d'une adaptation constante.

Le cycle classique du renseignement, bien que précieux à l'époque pour sa structure et sa normalisation, présente des limites importantes pour relever les défis contemporains, en particulier dans le domaine numérique. La nature dynamique et décentralisée du cyberspace, ainsi que le volume et la vitesse des données, exigent des modèles plus souples et plus adaptatifs. Le modèle IDEM proposé dans le présent document répond à ce besoin au moyen d'une structure modulaire, non linéaire et en réseau, où les phases interagissent simultanément et se nourrissent constamment les unes des autres.

Cette nouvelle approche réorganise les étapes du cycle traditionnel et ajoute des éléments clés tels que l'identification proactive des menaces, la contextualisation intégrée à l'analyse, la diffusion précoce et transversale du renseignement et l'intégration systématique du retour d'information. Elle intègre également des technologies avancées telles que l'intelligence artificielle et l'apprentissage automatique afin d'optimiser la gestion de grands volumes de données et d'améliorer les capacités prédictives.

Cependant, la technologie seule ne suffit pas. Le jugement humain, la capacité critique, la créativité analytique et la connaissance du contexte restent essentiels. La synergie entre les analystes et les systèmes automatisés permet d'obtenir des renseignements plus efficaces, plus précis et plus utiles pour la prise de décision.

En bref, le renseignement du 21^e siècle doit être agile, multidisciplinaire et collaboratif. Seules des approches hybrides, ouvertes à l'apprentissage et à l'amélioration continue, permettront d'anticiper et d'atténuer efficacement les menaces émergentes. Le modèle IDEM est un pas dans cette direction : une proposition adaptative et réaliste pour relever les défis que l'ère numérique impose aux systèmes de renseignement contemporains.

La réalité du contexte actuel continue de présenter des défis et des difficultés considérables pour anticiper et atténuer efficacement les menaces contemporaines, en particulier celles qui se manifestent dans le cyberspace, car il est difficile de suivre et de devancer les cybercriminels. Il est donc nécessaire que la communauté du renseignement continue à rechercher et à développer des stratégies qui réduisent les faiblesses actuelles, favorisent la sensibilisation à la culture du renseignement, la diffusion de l'information et la coopération internationale.

6. RÉFÉRENCES BIBLIOGRAPHIQUES

- Andric, J. et Terzic, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. *Journal of Information Systems & Operations Management*, 17(1). <https://doi.org/10.1080/2158379X.2021.1879572>
- Atwood, C. P. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis (Le renseignement basé sur les activités révolutionne l'analyse du renseignement militaire). *Joint Force Quarterly*, 77. <https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/>
- Budhram, T. (2015). Intelligence-led policing : A proactive approach to combating corruption. *South African Crime Quarterly*, 52. <https://doi.org/10.17159/2413-3108/2015/i52a30>
- Carter, J. G. et Fox, B. (2019). Community policing and intelligence-led policing : An examination of convergent or discriminant validity. *Policing : An International Journal*, 42(1), 43-58. <https://doi.org/10.1108/PIJPSM-07-2018-0105>
- Centre national de cryptologie (2015). CCN-STIC-425 Cycle de renseignement et d'analyse d'intrusion.
- National Intelligence Centre (2023). Origines des services de renseignement. <https://www.cni.es/sobre-el-cni/nuestra-historia>
- Chainey, S. et Chapman, J. (2013). A problem-oriented approach to the production of strategic intelligence assessments. *Policing : An International Journal of Police Strategies & Management*, 36(3), 474-490. <https://doi.org/10.1108/PIJPSM-02-2012-0012>
- Dahj, J. N. M. (2022). Maîtriser la cyber-intelligence. Packt Publishing Ltd.

- Díaz Fernández, A. M. (2013). Le rôle de l'intelligence stratégique dans le monde d'aujourd'hui. Cuadernos de Estrategia, 162, 35-66. <https://dialnet.unirioja.es/servlet/articulo?codigo=4275959>
- Francisco, J., & Barrilao, S. (2019). Services de renseignement, secret et garantie judiciaire des droits. Teoría y Realidad Constitucional, 309-340.
- Gkougkoudis, G., Pissanidis, D. et Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143-163. <https://doi.org/10.3390/digital2020009>
- Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).
- Gruszczak, A. (2018). Le défi de l'adaptation des services de renseignement de l'OTAN. <https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge>
- Jefatura del Estado (2002). Loi 11/2002, du 6 mai, régissant le Centre national d'intelligence.
- Jiménez Villalonga, R. (2018, 26 novembre). Les types d'intelligence. <https://global-strategy.org/tipos-de-inteligencia/>
- Jordán, J. (2011). Introduction à l'analyse du renseignement. 2340-8421, 2, Art. 2. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Jordán, J. (2016). Un examen du cycle du renseignement. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. <https://www.seguridadinternacional.es/resi/index.php/revista>
- Kamiński, M. A. (2019). Les sources de renseignement dans le processus de collecte d'informations par la communauté du renseignement des États-Unis. Security Dimensions, 32(32), 82-105. <https://doi.org/10.5604/01.3001.0014.0988>
- Knight, T. C. (2024). Five Thousand Candles : Optimizing Information Sharing Policies for Homeland Security (Cinq mille bougies : optimisation des politiques de partage de l'information pour la sécurité intérieure). Système universitaire public américain.
- Lee, M. (2023). Cyber Threat Intelligence (1ère éd.), John Wiley & Sons, Inc.
- Mahood, L. M. E. K. (2015). SOCMINT : suivre et aimer le renseignement sur les médias sociaux [Collège des Forces canadiennes]. <https://www.cfc.forces.gc.ca/254-eng.html>.

- Ministère de la défense (2023). Renseignement, surveillance et reconnaissance.
- Montero Gómez, A. (2006). Inteligencia Prospectiva de Seguridad (24 ; domaine : sécurité et défense). <https://www.realinstitutoelcano.org/publicaciones/>
- Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51-66. <https://dialnet.unirioja.es/servlet/articulo?codigo=2270935>
- Navarro Bonilla, D. (2005). Information, espionnage et renseignement dans la monarchie hispanique (XVIe-XVIIe siècles). *Revista de Historia Militar, Extraordinario*, 13-40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075
- Organisation pour la sécurité et la coopération en Europe (2017). Guide de l'OSCE sur la police fondée sur le renseignement (Département des menaces transnationales, Unité des questions stratégiques de police, Ed. ; Vol. 13).
- Payá-Santos, C. A. (2023). Les performances de l'intelligence en Espagne dans les sphères publiques, commerciales et académiques. *Revista Científica General José María Córdova*, 21(44), 1029-1047. <https://doi.org/10.21830/19006586.1222>
- Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). *Understanding the Intelligence Cycle* (M. Phythian, Ed.).
- Portillo, I. (2019). Savoir ce que sont la cyberveille et le renseignement sur les cybermenaces. <https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/>
- Pothoven, S., Rietjens, S. et de Werd, P. (2023). Producer-client paradigms for defense intelligence. *Defence Studies*, 23(1), 68-85. <https://doi.org/10.1080/14702436.2022.2089658>
- Stewart Bertram (2015). *Le Tao de l'intelligence Open Source*. IT Governance Publishing.
- Summers, L. et Rossmo, D. K. (2019). Offender interviews : implications for intelligence-led policing. *Policing*, 42(1), 31-42. <https://doi.org/10.1108/PIJPSM-07-2018-0096>
- Vela Tejada, J. (1993). Tradition et originalité dans l'œuvre d'Énée le tacticien : la genèse de l'historiographie militaire. *Minerva. Revista de Filología Clásica*, 7, 79-92. <https://doi.org/https://doi.org/10.24197/mrfc.7.1993>



Article de recherche

HACKTIVISME : DE LA PROTESTATION SOCIALE À L'INSTRUMENTALISATION DE L'ÉTAT

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

Josué Expósito Guisado

Sergent de la Guardia Civil

Doctorant à l'Université Pablo de Olavide

Maîtrise en paix, sécurité et défense par l'Institut de recherche sur la paix, la sécurité et la défense.

Institut universitaire Gutiérrez Mellado (UNED)

jexpgui@gmail.com

ORCID : 0009-0003-4977-3899

Reçu le 18/03/2025

Accepté le 05/05/2025

Publié le 27/06/2025

Citation recommandée : Expósito, J. (2025). Hactivisme : de la protestation sociale à l'instrumentalisation de l'État. *Logos Guardia Civil Magazine*, 3(2), pp. 101-122.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

HACKTIVISME : DE LA PROTESTATION SOCIALE À L'INSTRUMENTALISATION DE L'ÉTAT

Résumé : INTRODUCTION. 2. DE LA PROTESTATION SOCIALE À LA CYBERGUERRE. 3. 3. LE LIEN ENTRE HACKTIVISME ET APT. 4. L'AVENIR DES GROUPES HACKTIVISTES. 5. CONCLUSIONS. 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : L'hacktivism est passé d'une forme initiale de protestation numérique à un outil clé dans les conflits géopolitiques contemporains. Ce qui a commencé comme un mouvement décentralisé de défense de la liberté d'expression et de la justice sociale a été progressivement instrumentalisé par les Etats pour exécuter des cyber-attaques, manipuler l'opinion publique et déployer des opérations de désinformation. Ce phénomène s'est particulièrement accentué dans le contexte de la guerre en Ukraine, où la convergence entre les groupes APT (Advanced Persistent Threat) et les hacktivistes patriotes a permis l'exécution d'opérations cybernétiques coordonnées avec les intérêts de l'État. Parallèlement, l'internationalisation de l'hacktivism a conduit à la formation d'alliances entre des groupes de différentes régions, élargissant ainsi son impact au-delà du conflit russo-ukrainien. Le cyberspace s'est imposé comme une arène idéale pour la confrontation entre États dans un environnement contrôlé. Toutefois, la sophistication croissante des attaques et le ciblage de plus en plus stratégique posent de sérieux défis à la stabilité internationale et à la sécurité des États occidentaux.

Resumen: El hacktivismo ha evolucionado desde una forma inicial de protesta digital hasta convertirse en una herramienta clave en los conflictos geopolíticos contemporáneos. Lo que comenzó como un movimiento descentralizado en defensa de la libertad de expresión y la justicia social, ha sido progresivamente instrumentalizado por los Estados para ejecutar ciberataques, manipular la opinión pública y desplegar operaciones de desinformación. Un fenómeno que se ha visto especialmente acentuado en el marco de la guerra de Ucrania, donde la convergencia entre grupos de Amenaza Persistente Avanzada (APT) y hacktivistas patrióticos ha permitido la ejecución de operaciones cibernéticas coordinadas con los intereses estatales. Paralelamente, la internacionalización del hacktivismo ha llevado a la formación de alianzas entre grupos de distintas regiones, ampliando su impacto más allá del conflicto ruso-ucraniano. El ciberespacio se ha consolidado como un escenario idóneo para la confrontación entre Estados en un entorno controlado. Sin embargo, la creciente sofisticación de los ataques y la selección de objetivos cada vez más estratégicos plantean serios desafíos a la estabilidad internacional y la seguridad de los Estados occidentales.

Mots-clés : Hacktivism, APT, cyberproxies, cyberconflits, cyberattaques.

Palabras clave: Hacktivismo, APT, ciberproxies, ciberconflicto, ciberataques.

ABBREVIATIONS

APT : *Advanced Persistent Threat (menace persistante avancée).*

DDoS : *attaque par déni de service distribué.*

DOJ : *Département de la justice des États-Unis.*

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

GRU : *Direction principale du renseignement de la Russie (Glavnoe Razvedyvatel'noe Upravlenie).*

ICS : *Industrial Control Systems (systèmes de contrôle industriel).*

IRGC : *Corps des gardiens de la révolution islamique d'Iran.*

IT Army of Ukraine : *IT Army of Ukraine.*

NSA : *Agence nationale de sécurité des États-Unis.*

PMC : *Private Military Company (société militaire privée).*

PSOA : *Private Sector Offensive Actor (acteur offensif du secteur privé).*

SCADA : *Supervisory Control And Data Acquisition (contrôle de surveillance et acquisition de données).*

Stuxnet : *nom du logiciel malveillant utilisé dans l'opération "Jeux olympiques".*

1. INTRODUCTION

Avec la guerre en Ukraine, le monde occidental est à nouveau confronté à l'impact du réalisme politique. Avant l'invasion de 2022, la grande majorité des analystes occidentaux étaient incapables d'envisager un conflit conventionnel sur la scène internationale tel que celui qui continue de se produire aux portes de l'Europe. Aveuglés par les doctrines de soft power et suivant les paradigmes libéraux de la paix capitaliste ou de la théorie de la paix commerciale, les dirigeants européens ont volontairement ignoré le fait que dans certaines parties du monde, le réalisme politique règne toujours en maître.

Dans un monde de plus en plus numérisé, où il existe une interconnexion virtuelle entre le plan intangible des technologies de l'information et l'espace physique lui-même, il n'est pas surprenant que l'ennemi actuel de l'Europe pose un problème de sécurité. Les États étant de plus en plus dépendants des technologies de l'information, les acteurs hostiles (étatiques et non étatiques) ont de plus en plus de possibilités d'influencer l'environnement politique et géopolitique en déployant des actions dans le cyberspace.

La guerre en Ukraine a non seulement marqué le début d'une opération de harcèlement et de cyberperturbation par des cybermenaces liées au Kremlin, mais elle a également entraîné un changement dans le paysage mondial de l'hactivisme : ce qui, il n'y a pas si longtemps encore, était le bastion de la défense de la liberté d'expression, de la vie privée, de la justice sociale et des droits de l'homme, est aujourd'hui un outil aux implications stratégiques et, dans de nombreux cas, lié directement ou indirectement à des gouvernements et à des services de renseignement.

L'activisme numérique idéologique et protestataire que représentait autrefois Anonymous évolue vers un phénomène composé d'une myriade de groupes nationalistes qui utilisent de manière répétée les attaques par déni de service distribué (DDoS) pour créer un climat de tension et un harcèlement persistant des ennemis occidentaux.

L'hactivisme est devenu un outil à double tranchant. D'une part, il représente une forme d'expression et de lutte pour la justice sociale, la transparence et les droits de l'homme. D'autre part, il est devenu une arme utilisée par les États pour déployer des campagnes de déstabilisation politique et de désinformation.

L'utilisation de cyberattaques à des fins géopolitiques a mis en évidence la frontière ténue entre l'activisme et la cybercriminalité parrainée par l'État. Cet article vise à analyser l'évolution de l'hactivisme et ses relations avec les gouvernements, ainsi que le rôle des groupes de menaces persistantes avancées (APT) dans l'utilisation du cyberspace à des fins politiques et militaires .¹

À travers l'examen de cas concrets, il explorera la collaboration (ou l'instrumentalisation) des hacktivistes par les États, les implications de cette pratique et son impact sur la géopolitique actuelle. Enfin, une réflexion sera proposée sur l'avenir de

¹ Groupes de cyber-attaquants souvent associés à des États-nations ou à de grandes organisations criminelles, très sophistiqués et persistants, qui infiltrent des réseaux pendant de longues périodes à des fins d'espionnage ou de sabotage et qui disposent d'abondantes ressources (techniques, économiques) pour attaquer des cibles de grande valeur (gouvernements, grandes entreprises) avec préméditation et furtivité.

l'hacktivisme dans un monde de plus en plus interconnecté, où l'intelligence artificielle et d'autres technologies émergentes pourraient redéfinir le rôle de ces acteurs dans le cyberspace.

L'hacktivisme n'est plus seulement un phénomène marginal de protestation numérique, mais un risque potentiel pour la sécurité des États. Il est essentiel de comprendre son évolution et ses implications pour analyser l'avenir de la cybersécurité espagnole.

2. DE LA PROTESTATION SOCIALE À LA CYBERGUERRE

L'hacktivisme a subi une transformation remarquable depuis ses origines, passant d'une forme de protestation sociale à un outil utilisé par les gouvernements pour soutenir un agenda politique. Si l'on y réfléchit bien, cette transformation trahit les origines et l'essence même de l'activisme. C'est pourquoi, avant d'analyser le rôle joué par l'hacktivisme en tant qu'outil au service de l'État, nous pensons qu'il est nécessaire d'examiner l'évolution de ce phénomène depuis ses origines.

Dans certaines approches contemporaines, en particulier celles qui sont axées sur la systématisation terminologique, il existe une tendance à établir une relation hiérarchique entre le cyberactivisme et l'hacktivisme, en considérant le premier comme un phénomène plus large et en englobant nécessairement le second comme une manifestation spécifique ou une variante radicalisée. Cette lecture, présente à la fois dans la littérature populaire et dans certains cadres analytiques normatifs, considère que le cyberactivisme représente l'utilisation des technologies numériques pour la promotion de causes sociales, politiques ou culturelles par le biais de campagnes de sensibilisation, de pétitions en ligne ou de protestations virtuelles. Le hacktivisme, quant à lui, se caractérise par l'utilisation d'outils de piratage informatique - tels que les attaques par déni de service distribué (DDoS), les violations de données ou la modification de sites web - à des fins similaires, mais par des moyens plus perturbateurs, voire illicites.

Cependant, cette interprétation, bien que largement répandue, est problématiquement réductrice et ne résiste pas à un examen plus approfondi de la théorie historique et critique des mouvements numériques. Premièrement, l'hypothèse d'une évolution linéaire et progressive - du cyberactivisme "modéré" à l'hacktivisme "radical" - ignore les trajectoires historiques distinctes des deux concepts. L'hacktivisme, loin d'être une dérivation tardive du cyberactivisme, émerge simultanément et même plus tôt dans certains contextes, enraciné dans la culture hacker des années 1980 et 1990, et articulé autour de principes tels que la liberté d'information, le libre accès à la connaissance et la désobéissance civile dans le cyberspace (Jordan & Taylor, 2004 ; Coleman, 2014).

En fait, le terme "hacktivisme" provient de la combinaison étymologique de "hacker" et "activism", décrivant l'utilisation de compétences informatiques pour promouvoir des causes politiques ou sociales ; ses racines remontent au milieu des années 1990, lorsque des groupes tels que le "*Cult of the Dead Cow*" (une référence à l'abattoir texan où le groupe tient ses réunions) ont défendu l'accès universel à l'information en

ligne comme un droit humain fondamental et la lutte contre les gouvernements oppresseurs.²

"*Cult of the Dead Cow*, considéré comme l'un des fondateurs de l'hactivisme moderne, a non seulement diffusé des manifestes critiquant le contrôle de l'Internet par l'État et les entreprises, mais a également mis au point des outils à vocation clairement perturbatrice. Parmi eux, *Back Orifice* (1998), un logiciel conçu pour exposer les vulnérabilités du système d'exploitation Windows et dénoncer les lacunes des utilisateurs en matière de protection de la vie privée³. Un an plus tard, en 1999, plusieurs de ses membres ont promu le projet *Hactivismo*, une branche explicitement orientée vers la lutte contre la censure numérique qui a donné lieu au développement d'outils tels que *Six/Four* ou *Peekabooby*, conçus pour contourner les filtres imposés par les régimes autoritaires et faciliter le libre accès à l'information.

Dans l'idéologie du *Culte de la Vache Morte*, l'accès à l'information en ligne n'est pas seulement un droit fondamental, mais aussi un champ de contestation politique qui exige des formes innovantes d'intervention technique et symbolique. Cependant, ces actions, bien que non violentes sur le plan physique, impliquent une confrontation directe avec la législation restrictive sur l'utilisation des réseaux et la propriété intellectuelle ; en d'autres termes, elles révèlent le caractère ambigu de l'hactivisme.

D'autre part, conceptualiser l'hactivisme comme une simple intensification tactique du cyberactivisme nous fait perdre de vue les divergences idéologiques et épistémologiques entre les deux. Alors que le cyberactivisme tend à s'inscrire dans une logique de participation citoyenne, de plaidoyer institutionnel et d'utilisation stratégique des médias sociaux, l'hactivisme opère souvent sur la base d'un antagonisme direct, d'une résistance aux structures de pouvoir et d'une remise en question des cadres juridiques existants.

S'il peut être utile de considérer l'hactivisme comme une sous-catégorie du cyberactivisme selon certaines approches descriptives, cette approche est épistémologiquement insuffisante et empiriquement discutable lorsqu'il s'agit d'aborder la généalogie, le cadre normatif et les implications éthico-politiques de ces deux formes d'activisme numérique. Dans cet article, nous nous concentrerons uniquement sur l'évolution de l'hactivisme, compris comme un phénomène à part entière, en laissant de côté la formulation d'un examen critique de cette classification.

Dans les premiers temps de l'hactivisme, l'objectif principal était de mener des attaques contre les gouvernements et les entreprises pour protester contre la censure et les injustices sociales. Ces messages se sont intensifiés lorsque le mouvement anti-mondialisation du milieu des années 1990 est apparu sur la scène sociale (Auty, 2004).

La guerre du Kosovo dans les années 1990 (souvent décrite comme la première guerre menée en ligne) a constitué une étape clé dans la consolidation de l'hactivisme en tant qu'outil d'affrontement politique : les belligérants ont non seulement partagé des

² Le site web de "The Cult of the Dead Cow" peut toujours être consulté à l'adresse suivante : <https://cultdeadcow.com/about.html>

³ Bien que conçu à l'origine comme un outil d'audit de sécurité, sa création a suscité une certaine controverse et a été perçue comme une menace par l'industrie technologique.

informations et des témoignages sur la guerre en ligne, mais ils ont également diffusé de la propagande et de la désinformation. *Des pirates informatiques* sont même apparus et sont intervenus activement dans le conflit en défigurant des sites web gouvernementaux et en exécutant des attaques par déni de service contre les infrastructures en ligne de la partie adverse (Denning, 2001).

Sur le plan académique et social, les mouvements hacktivistes ont été perçus comme l'expression naturelle d'un activisme politique préexistant qui avait trouvé dans un nouvel outil (Internet) la possibilité d'employer un type d'activiste au profil technique pour diffuser ses messages d'une manière plus médiatique (Jordan, 2002).

Cependant, le mépris manifeste des normes établies, les noms choisis par les groupes (*The Legion of Doom*, *Bad Ass Mother Fuckers*, *Toxic Shock*, etc.) et le contexte d'insécurité sociale ouvert par les attentats du 11 septembre 2001 ont fait qu'un phénomène initialement perçu positivement a commencé à susciter une certaine méfiance (Torres Soriano, 2018).

La figure du *hacker* a commencé à être identifiée à celle du criminel et, par extension, dans un contexte géopolitique marqué par la lutte contre la Terreur, à celle du cyberterroriste. Et les actions hacktivistes ont commencé à être identifiées fondamentalement comme une nouvelle forme de participation politique illégitime, utilisant les cyber-attaques pour effectuer du sabotage et du cyber-espionnage (Vegh, 2005).

Au niveau académique, l'identification de l'hacktivisme à l'illégal ou au criminalisable, fréquente dans certains discours, réduit l'hacktivisme à une "forme radicale de cyberactivisme", et appauvrit ainsi la capacité d'analyse et d'explication des sciences sociales face à la complexité des pratiques politiques numériques contemporaines.

Les débuts de cette décennie reflètent un hacktivisme marqué par la volonté de ses membres de transgresser les conventions sociales pour le plaisir. En effet, les racines du groupe hacktiviste le plus connu (Anonymous) remontent au forum japonais *2chan*, où la communauté virtuelle était dédiée au partage de toutes sortes de contenus aberrants liés à l'anime, au porno et aux blagues (Bartlett, 2015).

Cependant, vers 2003, les premières tensions internes sont apparues au sein d'une communauté virtuelle qui avait trouvé dans le forum *4chan* un endroit idéal pour s'amuser sans se soucier des conséquences. C'est précisément dans ce forum que certains utilisateurs (connus sous le nom de *moralfags*) ont proposé de concentrer leurs activités sur des causes plus transcendantes telles que la lutte contre la censure sur Internet, afin d'assainir l'image de l'hacktivisme et de représenter la défense de la liberté d'expression, de la transparence et d'autres droits civils.

Sous le slogan "*Nous sommes anonymes. Nous sommes la Légion. Nous ne pardonnons pas, nous n'oublions pas. Attendez-vous à nous*" et le masque de Guy Fawkes, un collectif décentralisé d'activistes a vu le jour, combinant l'exfiltration d'informations et les attaques DDoS pour justifier la lutte contre la corruption, la censure et les abus de pouvoir.

Du côté du pouvoir en place, Anonymous a rapidement été interprété comme une prémonition du risque posé par une nouvelle génération d'acteurs virtuels motivés, avec une structure sans leader et un fonctionnement basé sur le volontarisme et la spontanéité (Olson, 2012). Cependant, ce n'est que lorsque le collectif a commencé à soutenir les actions de WikiLeaks que le groupe a été perçu comme une cybermenace de premier plan.

En peu de temps, les Anonymous sont passés d'un petit groupe de *hackers* à l'esprit politique à un mouvement mondial comptant des milliers d'adeptes dans le monde entier. Cependant, leur attrait ne réside pas dans une idéologie structurée ou un programme d'action défini. Au-delà de leur position anti-establishment, qui les a amenés à dénoncer la manipulation et le contrôle exercés par les gouvernements et les entreprises, leur philosophie manquait d'une orientation claire sur la manière dont la politique, la société ou l'économie devraient être organisées. Cela a fait des Anonymous un phénomène difficile à cerner, car leur identité reposait davantage sur l'action et la protestation que sur un programme concret de changement (Torres Soriano, 2018).

Sous le masque de Guy Fawkes se sont rassemblés des individus qui croyaient certainement soutenir un changement social positif, mais aussi d'autres : ceux dont l'inspiration était la destruction nihiliste du monde tel que nous le connaissons et ceux qui cherchaient à se cacher sous la bannière d'Anonymous pour en tirer un profit politique ou économique.

Le principal héritage d'Anonymous, qui a fait de l'hacktivismisme une pratique populaire transcendant la sphère des *hackers*, a donné naissance à une nouvelle ère d'hacktivistes opérant dans un paysage fragmenté et complexe, où coexistent de multiples acteurs aux motivations diverses.

Aujourd'hui, si des groupes comme Anonymous continuent d'opérer de manière décentralisée, leur impact a diminué par rapport à l'essor qu'ils ont connu au début des années 2010. Dans le même temps, de nouvelles générations d'hacktivistes sont apparues, qui, bien qu'ayant un niveau d'expertise technique inférieur, compensent par l'utilisation d'outils d'automatisation et une maîtrise de l'impact médiatique et de la mobilisation sociale.

Aujourd'hui, l'hacktivismisme est utilisé à la fois par des collectifs indépendants dénonçant l'injustice et par des groupes parrainés par l'État qui instrumentalisent ces tactiques à des fins géopolitiques. Le conflit entre la Russie et l'Ukraine a mis en évidence l'existence d'une cyberguerre, les hacktivistes pro-ukrainiens et pro-russes menant des attaques coordonnées au profit de leur camp respectif.

La frontière entre l'activisme numérique légitime, la cybercriminalité et les opérations secrètes de renseignement est de plus en plus floue. Cependant, nous pouvons considérer qu'il existe actuellement trois types d'hacktivistes : les cyberterroristes, les *hackers* civiques et les *hackers* patriotiques (Dahan, 2013 ; Denning, 2001 ; Johnson et Robinson, 2014 ; Sauter, 2013).

Le cyberterrorisme comprendrait toutes les actions hostiles dans le cyberspace visant à perpétrer des actes de violence contre des personnes ou des biens, dans le but d'intimider ou de contraindre des gouvernements ou des sociétés à atteindre des objectifs politiques, religieux ou idéologiques spécifiques. Ces actions consistent principalement à

diffuser des virus et des *logiciels malveillants*, à vandaliser des *sites web* et à mener des attaques par déni de service (DDoS) ou par *botnet* (Denning, 2001 ; Jordan et Taylor, 2004 ; Goode, 2015).

Dans la catégorie des *hackers* civiques, on trouve tous les groupes organisés qui mènent des actions contre des systèmes informatiques dans le but d'apporter une contribution à la communauté, généralement à la limite de la légalité (Hunsinger et Schrock, 2016 ; Schrock, 2016).

Enfin, les *hackers* patriotiques sont des individus ou des groupes dont les efforts sont alignés sur l'idéologie nationaliste et qui sont considérés comme une "cyber-milice" à la poursuite d'intérêts spécifiques (Dahan, 2013 ; Green, 2016). Même si, de l'extérieur, ces *hackers* ne semblent pas être directement parrainés par un État, nous pouvons désormais en déduire qu'ils sont instrumentalisés dans le cadre d'un réseau plus large de forces étatiques.

Le *piratage informatique* patriotique a vu le jour en Chine dans les années 1990 en réponse aux émeutes anti-chinoises en Indonésie, et a depuis été utilisé comme tactique par la Chine, la Russie, la Syrie et d'autres États pour nuire à leurs ennemis dans le domaine cybernétique. Toutefois, aucune des opérations antérieures à la guerre d'Ukraine n'a eu l'ampleur, l'impact et les liens gouvernementaux aussi solides et prolongés, ni n'a transgressé les normes internationales de manière aussi flagrante que l'hacktivisme contemporain (Healey & Grinberg, 2022).

3. LE LIEN ENTRE L'HACKTIVISME ET L'APT

Tout au long de l'histoire, les États ont eu recours à des acteurs de substitution pour mener à bien leurs stratégies de conflit sans engager directement leurs forces armées. Unités auxiliaires, groupes mercenaires, insurrections, organisations terroristes ou sociétés militaires privées (SMP) ne sont que quelques-unes des formes que les acteurs tiers ont prises pour se substituer à l'action stratégique des États.

Il n'est donc pas surprenant qu'aujourd'hui, dans une société de plus en plus numérisée, l'État ait trouvé dans les groupes hacktivistes un nouvel acteur pour personifier l'externalisation de la paternité, et dans le cyberspace, l'environnement idéal pour projeter une influence géopolitique.

Le concept de *guerre de substitution* a fait l'objet d'un débat approfondi au sein de la communauté universitaire et de la communauté de la sécurité, notamment en raison de la difficulté à le différencier de la guerre *par procuration*, étant donné la nature étroitement liée des deux concepts.

Dans les deux cas, les objectifs de l'acteur principal (l'État) et de l'agent mandataire coïncident. Cependant, alors que dans la *guerre par procuration* il y a deux ou plusieurs acteurs hiérarchiquement liés (l'acteur principal travaille pour, avec et par l'intermédiaire de l'acteur mandataire pour atteindre un objectif commun), dans la *guerre de substitution* ces acteurs ne sont alignés que si l'acteur principal est en mesure de mobiliser le soutien adéquat requis par l'acteur mandataire (Fox 2019). En d'autres termes, les concepts de *guerre de substitution* et de *guerre par procuration* diffèrent en fonction de la relation entre les acteurs et de leurs motivations.

Étant donné que les groupes hacktivistes ont peu d'indépendance pour résister au contrôle de l'État qui les sponsorise (ou du moins les influence ou les tolère), nous parlerons dans notre étude de cas d'acteurs *par procuration*.

Plus précisément, pour les désigner, nous utiliserons la définition des " *proxy actors* " de Rondeaux et Sterman (2019), qui les définissent comme des " *sujets extérieurs à la structure de sécurité des États impliqués dans un conflit qui agissent sous le parrainage direct ou indirect d'un acteur conventionnel (un État)* " ; et la définition des *cyberproxies* de Maurer (2018) comme des " *intermédiaires qui mènent des actions offensives dans le cyberspace au profit d'un acteur principal* ".

Historiquement, les *cyberproxies* ont été personnifiées par diverses entités liées au monde de la cybercriminalité et du cyberespionnage. Cependant, le terme englobe un grand nombre d'entités organisées qui, directement ou indirectement, représentent un facteur de risque pour les entreprises et les États. En fait, la liste des acteurs est très longue : groupes criminels, *acteurs offensifs du secteur privé* (PSOA), groupes terroristes, insurgés, hacktivistes, acteurs étatiques ou APT n'en sont que quelques-uns.

Les raisons de leur utilisation sont diverses : (1) l'utilisation d'acteurs *mandataires* par les gouvernements réduit le risque d'escalade des conflits, car il est difficile d'attribuer la responsabilité d'une cyber-attaque ; (2) il existe une possibilité de déni plausible qui détourne la responsabilité d'une attaque vers un acteur échappant au contrôle du gouvernement ; (3) elle aide les États à prolonger la situation de tension dans les conflits en épuisant leur adversaire sur le plan social, politique et économique ; (4) elle permet aux États d'agir en dehors des réglementations nationales et des critiques des secteurs gouvernementaux opposés - voire de l'opinion publique elle-même dans les démocraties ; (5) elle permet aux États de réagir rapidement et avec souplesse aux actions offensives de leurs adversaires, car elle ne nécessite pas de preuves techniques ni de légitimation publique ; (6) elle offre aux États un outil de dissuasion supplémentaire ; (7) elle permet aux États de contourner l'application du droit international ; (8) elle facilite l'utilisation de personnel expert sans qu'il soit nécessaire de proposer un recrutement légal ; (9) elle permet de participer à des conflits internationaux qui seraient autrement économiquement et politiquement ingérables (Torres Soriano, 2017 ; Expósito Guisado, 2024 ; Marín Gutiérrez, 2023).

Cependant, l'obtention de ces avantages n'est pas sans poser de problèmes. En effet, le principal attrait de l'utilisation d'un *proxy* (qui n'est autre que l'obtention d'un déni plausible d'une agression) est aussi sa principale faiblesse, car l'anonymat et la clandestinité diluent la capacité coercitive et dissuasive de l'État commanditaire - après tout, nous ne pouvons ignorer les théories de Clausewitz qui suggèrent que pour qu'un État modifie sa conduite en fonction de la volonté d'un autre, ce dernier doit connaître l'origine de l'acte de coercition subi.

Un autre inconvénient de l'utilisation des *cyberprocurations* réside dans la manière dont l'État les sélectionne et les contrôle lorsqu'elles sont utilisées. L'existence d'intérêts divergents entre les deux parties peut conduire à la déloyauté du *proxy*, causant des dommages économiques ou politiques à l'acteur qui les utilise - un fait qui est aggravé si l'on tient compte du fait que ces *proxys* opèrent généralement dans des zones où l'État ne peut ni ne veut intervenir.

L'avantage des *mandataires* réside dans leur capacité à agir secrètement, mais c'est justement ce manque de transparence qui empêche l'État commanditaire de vérifier leurs antécédents et leur fiabilité. La littérature académique souligne que le contrôle des *mandataires* est encore plus compliqué si l'État ne dispose pas de mécanismes efficaces pour sanctionner la déloyauté, ou s'il existe des structures décentralisées qui empêchent l'application correcte des ordres hiérarchiques (Popovic 2015).

Dans cet article, nous nous concentrerons uniquement sur deux acteurs qui représentent les deux pôles différents (activisme ouvert et espionnage silencieux) d'un même phénomène, mais qui ne sont pas si différents en termes d'objectifs qu'ils poursuivent et d'instrumentalisation de ces derniers par les États.

D'une manière générale, l'hacktivisme et les APT se distinguent par leurs motivations, leurs méthodes et le degré de soutien de l'État. Ainsi, alors que l'hacktivisme est motivé par un contexte socio-politique (protestation, activisme, causes morales), les APT se concentrent sur l'espionnage stratégique et l'obtention d'un avantage économique et militaire.

Sur le plan opérationnel, les APT agissent de manière furtive et persistante, en utilisant des *logiciels malveillants* personnalisés, des portes dérobées et des mouvements latéraux, contrairement aux actions des hacktivistes qui cherchent généralement à attirer l'attention du public et se concentrent généralement sur des attaques DDosS à court terme.

Cependant, il n'est pas rare d'observer comment les APT agissent temporairement comme des hacktivistes (lorsqu'ils divulguent publiquement les données qu'ils exfiltrent pour provoquer un impact politique) et comment les hacktivistes sont instrumentalisés par les États pour atteindre leurs objectifs stratégiques.

Au niveau organisationnel, les hacktivistes et les APT diffèrent également : les hacktivistes agissent généralement de manière décentralisée, spontanée, voire anonyme, et sans commandement unifié. Les APT, en revanche, sont généralement des équipes structurées, souvent intégrées dans une organisation plus vaste (une armée, une agence de renseignement ou un groupe criminel), avec une hiérarchie définie et un financement nettement plus puissant (CyberZaintza, 2021).

En effet, la différence de ressources et de formation technique suggère un lien plus étroit entre les APT et les États qu'avec les groupes hacktivistes. Toutefois, la frontière entre les deux concepts a récemment été brouillée par la prise de conscience que certains groupes hacktivistes pro-russes recevaient un soutien secret de l'État ou agissaient conformément à l'agenda de l'État, brouillant ainsi la distinction jusqu'alors claire entre les "*hackers* activistes" et les "agents de l'État" (Muncaster, 2024).

En fait, il n'est pas exclu que certains groupes d'hacktivistes soient formés ou soutenus par des APT ou directement par des acteurs étatiques. C'est le cas par exemple de "XakNet Team", "Infocentr" et "CyberArmyofRussia_Reborn", des groupes hacktivistes pro-russes qui, selon Mandiant, sont des acteurs de la cybermenace parrainés par la Direction principale du renseignement russe (GRU) par l'intermédiaire de l'APT44 (Mandiant, 2022).

Au cours de la dernière décennie, de nombreux cas ont été documentés dans lesquels des États ont utilisé à la fois leurs propres groupes APT et des collectifs d'hacktivistes (ou leurs identités) pour mener des opérations de cyberespionnage, de sabotage de conflits et de manipulation politique.

Un exemple paradigmatique illustrant l'interdépendance de ces deux concepts se trouve dans les élections américaines de 2016, lorsque "*DCLeaks*" et "*Guccifer 2.0*", deux identités liées à la Direction principale du renseignement de la Russie (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), ont volé des courriels du Parti démocrate et les ont diffusés en se faisant passer pour des "hacktivistes américains patriotiques" (DOJ, 2018).

Dans le sillage de la guerre en Ukraine, il n'est pas rare de constater une interdépendance entre les hacktivistes russes et les APT, des groupes tels que *Killnet*, *NoName057(16)*, *Anonymous Sudan* qui ont attaqué des sites web gouvernementaux et des entreprises occidentales pour soutenir le discours du Kremlin montrent que, bien que ces groupes se qualifient d'"activistes spontanés", ils agissent de manière suspecte en coordination avec l'action de l'État russe (Van Der Walt, 2025).

Cependant, la Russie n'est pas le seul acteur étatique à employer des APT et des hacktivistes pour déployer sa puissance. D'autres États comme la Chine, la Corée du Nord ou l'Iran sont également accusés depuis des années de mener leurs activités offensives dans le cyberspace de cette manière.

Plus précisément, la Chine est accusée depuis des années de parrainer de vastes campagnes de cyberespionnage par l'intermédiaire d'unités militaires et de *pirates informatiques* rémunérés, tels que ceux du groupe APT1, considéré par Mandiant en 2013 comme l'unité 61398 de l'Armée populaire de libération de la Chine.

Les opérations APT chinoises ont tendance à se concentrer sur des cibles stratégiques (aérospatiale, énergie, télécommunications, défense, etc.) et sont considérées comme faisant partie des services de renseignement de l'État chinois, mais contrairement à la Russie, l'utilisation de l'hacktivisme n'est pas aussi importante dans les stratégies chinoises.

Le gouvernement a toléré et même inspiré des "*hackers* patriotiques" chinois dans certains conflits, par exemple le "*Honker Hacker Network*", une communauté de *hackers* échappant au contrôle du gouvernement - selon des sources chinoises - qui a attaqué des acteurs adverses de la Chine lors de différends territoriaux ou d'incidents diplomatiques.

L'Iran, quant à lui, a montré une tendance à instrumentaliser des groupes de *hackers* prétendument activistes pour mener des opérations de représailles contre ses adversaires, tout en développant ses propres APT. Les attaques DDoS contre des banques américaines en 2012-2013, en représailles aux sanctions occidentales, en sont un exemple significatif : une entité se réclamant de l'hacktivisme religieux et s'appelant les "*Cyber Fighters of Izz ad-Din al-Qassam*" a revendiqué l'offensive, invoquant l'indignation suscitée par une vidéo anti-islamique (CFR, 2012).

Les agences de renseignement américaines ont ensuite conclu qu'il s'agissait d'une opération orchestrée par l'Iran (probablement ses gardiens de la révolution) en réponse aux mesures prises à l'encontre de son programme nucléaire. En fait, en 2016, le ministère

américain de la justice a inculpé sept Iraniens liés au Corps des gardiens de la révolution islamique (CGRI) pour ces attaques.

Un autre exemple est l'attaque "*Shamoonj*" menée en 2012 par le "*Cutting Sword of Justice*", un groupe hacktiviste présumé qui a effacé les données de 30 000 ordinateurs de la compagnie pétrolière saoudienne Aramco, mais que les analystes ont ensuite attribuée à une opération de l'État iranien en réponse à l'offensive *Stuxnet* et aux tensions régionales.

Malgré son isolement, la Corée du Nord a également réussi à créer l'une des cybermenaces les plus actives, principalement pour collecter des fonds et déstabiliser ses adversaires géopolitiques. Son groupe APT le plus connu, *Lazarus Group* (lié à APT38), a volé des centaines de millions en attaquant des banques.

Un autre cas illustrant l'instrumentalisation des campagnes militantes par les États peut également être trouvé dans l'une de leurs actions, le *piratage* de Sony Pictures en 2014, lorsqu'un groupe appelé "*Guardians of Peace*" a exfiltré des données confidentielles et détruit les systèmes de Sony en représailles apparentes au film satirique sur le dirigeant nord-coréen "*The Interview*". (FBI, 2014).

La Corée du Nord est le paradigme de l'instrumentalisation directe : ses *pirates informatiques* sont des agents de l'État qui prennent parfois le nom de groupes fictifs pour diffuser leurs messages ou justifier leurs attaques, mais contrairement à d'autres États, les Nord-Coréens ne font pas de distinction entre les APT et l'appareil d'État, ne gardant la couverture que dans le discours public destiné au monde extérieur.

Pour leur part, les puissances occidentales emploient manifestement aussi des capacités cybernétiques offensives pour attaquer d'autres États. Le cas le plus pertinent est sans doute l'opération "Jeux olympiques" attribuée aux agences de la NSA et à l'unité 8200 (officieusement reconnue), dans le cadre de laquelle les États-Unis et Israël ont développé le logiciel malveillant *Stuxnet* pour saboter les centrifugeuses nucléaires iraniennes vers 2010 (The Guardian, 2017).

En revanche, en Occident, s'il existe des entités APT soutenues par des États pour agir de manière offensive dans des campagnes d'espionnage, l'instrumentalisation de groupes hacktivistes pour masquer leurs actions est quasiment inexistante. En fait, on ne trouve qu'un seul cas où un groupe hacktiviste occidental lie son activité à la capacité cyber-offensive d'un État : l'"*Armée informatique de l'Ukraine*".

Ce cas est particulièrement controversé, car le soutien public du gouvernement ukrainien viole ouvertement les normes récemment adoptées sur la conduite des États dans le cyberspace, ainsi que les positions de politique étrangère des membres de l'OTAN (Healey et Grinberg, 2022).

Si nous utilisons le tableau "Spectre de responsabilité" de Healey et Grinberg (2022), qui établit une corrélation entre l'activité des groupes et le degré de responsabilité de l'État dans leur *cyberprocuration*, nous pouvons voir que le soutien du gouvernement ukrainien à l'*Armée de l'informatique de l'Ukraine* a commencé au moins comme "coordonné par l'État (niveau 6)", (lorsque le ministre ukrainien de la transformation numérique, Mikhaïl Fedorov, a ouvertement appelé les hacktivistes volontaires du monde

entier à soutenir l'Ukraine sur le front numérique) et même "encouragé par l'État (niveau 4)".

Tableau 1 : Spectre de la responsabilité de l'État.

Position de l'État	Relation entre l'État et le mandataire
1. Interdit par l'État.	Le gouvernement national contribuera à mettre fin à une attaque d'un tiers.
2. Interdiction de l'État, mais insuffisante.	Le gouvernement national coopère, mais il est incapables d'arrêter l'attaque des tiers.
3. Ignorée par l'État.	Le gouvernement national est conscient des attaques des tiers, mais n'est pas disposé à prendre aucune action officielle.
4. parrainé par l'État.	Des tiers contrôlent et dirigent l'attaque, mais le gouvernement national les promeut en tant que politique.
5. Façonné par l'État.	Des tiers contrôlent et dirigent l'attaque, et les L'État apporte un certain soutien.
6. Coordinné par l'État.	Le gouvernement national coordonne l'attaque en des tiers, par exemple en suggérant des détails opérationnel.
7. Obligation de l'État.	Le gouvernement national ordonne à des tiers de mener l'attaque en leur nom.
8. Géré, mais non reconnu par l'État.	Éléments échappant au contrôle des forces les attaques cybernétiques du gouvernement national conduisent à attaque ordonnée.
9. Mise en œuvre par l'État.	Le gouvernement national mène l'attaque en utilisant des forces cybernétiques sous leur le contrôle direct.
10. Intégrée à l'État.	Attaques des gouvernements nationaux à l'aide de mandataires intégrés et de cyberforces gouvernemental.

(Healey, 2022).

C'est surtout dans les conflits géopolitiques que l'on observe la convergence la plus accélérée entre l'hactivisme et les opérations étatiques. Dans le cas de la guerre en Ukraine, trois ans après le début du conflit et malgré le fait que le nombre d'acteurs hactivistes ait considérablement diminué (de plus de 130 groupes en 2024 à seulement environ 80 groupes en 2025), nous pouvons toujours observer comment les deux parties maintiennent un croisement de cyberattaques destructrices, coordonnées avec leur campagne militaire et soutenues dans leurs actions par des "hackers patriotiques" (Cyberknow, 2025).

Du côté ukrainien, l'*IT Army of Ukraine* reste la plus importante force hactiviste d'Ukraine, mobilisant toujours des volontaires à l'intérieur et à l'extérieur du pays pour attaquer l'infrastructure russe, mener des actions de contre-propagande et soutenir des missions de renseignement. Au cours de la période 2023-2024, on lui attribue, par

exemple, la coupure temporaire des services Internet dans les zones occupées par la Russie et le déploiement continu de campagnes DDoS contre des entités russes de premier plan (Optiv, 2023).

Du côté pro-russe, le groupe le plus en vue actuellement est *NoName057(16)*, un groupe lié au GRU, qui agit en coordination avec l'agenda du Kremlin en sélectionnant des cibles en accord avec les intérêts stratégiques russes et se considère comme une sorte de "bras cyber-spontané" permanent de l'armée russe.

Tableau 2 : Chronologie des cas d'instrumentalisation de l'hacktivisme par l'État.

<i>Année</i>	<i>État</i>	<i>Groupe hacktiviste</i>	<i>Fonctionnalité</i>	<i>Niveau de lien avec l'État (Healey & Grinberg).</i>
1998-1999	Kosovo	Pirates informatiques patriotes	Premier conflit avec une intervention hacktiviste notable.	Ignoré / Spontané
1999	Chine	Red Honker	Les pirates informatiques patriotiques actifs dans les conflits territoriaux. Campagnes d'espionnage industriel et cyber-attaques contre des infrastructures critiques.	Encouragé / Formé
2012-2013	L'Iran	Cybercom battants d'Izz ad-Din al-Qassam	Attaques DDoS contre des banques américaines en représailles aux sanctions. Opération Shamoon contre Aramco avec effacement massif.	Coordonné / ordonné
2014	Corée du Nord	Groupe Lazarus	Cyber-attaques pour le financement de l'État. Attaque contre Sony Pictures (2014) à titre de représailles symboliques.	Mis en œuvre / Intégré
2022-aujourd'hui	Russie	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Les groupes hacktivistes se sont coordonnés avec la stratégie russe dans la guerre en Ukraine. Attaques DDoS.	Coordonné / Encouragé

2022- aujourd'hui	Ukraine	Armée informatique de l'Ukraine	Appel public du gouvernement à l'hacktivisme contre la Russie. DDoS, sabotage et propagande pro- ukrainienne.	Coordonné / Encouragé
----------------------	---------	--	---	--------------------------

4. L'AVENIR DES GROUPES HACKTIVISTES.

La survie des groupes hacktivistes indique que l'hacktivisme intégré à la guerre est là pour durer, du moins tant que le conflit sous-jacent perdure et que les États en conflit trouvent ce niveau d'action décentralisée utile. En outre, le paysage actuel de l'hacktivisme nous amène à constater que l'hacktivisme va au-delà des DDoS et s'oriente vers des attaques APT plus sophistiquées, telles que les attaques contre les infrastructures critiques SCADA et les systèmes de contrôle industriel (ICS)⁴.

Le fait que des groupes appartenant à l'écosystème hacktiviste pro-russe, tels que *Z-Pentest Alliance* ou *Sector 16*, se soient activement introduits dans des centrales électriques, des installations d'eau potable et des industries en général, reflète non seulement une maturation et une étatisation du phénomène hacktiviste, mais aussi l'existence de risques physiques croissants de leurs actions (Antoniuk, 2024).

La réduction du nombre de groupes hacktivistes dans l'environnement pro-russe suggère que l'effervescence initiale a cédé la place à un processus de sélection naturelle dans lequel les groupes bénéficiant d'un meilleur soutien, d'une meilleure organisation et d'une meilleure protection survivent. Ce phénomène se traduit par des opérations plus efficaces et mieux coordonnées, mais aussi plus prévisibles car alignées sur l'agenda de l'État russe.

Dans le même temps, la persistance des attaques quotidiennes indique que la cyberguerre de basse intensité est devenue une routine. Les DDoS constants maintiennent une pression psychologique et de propagande sur les populations cibles (rappel quotidien de la présence d'un conflit), tandis que l'adoption de *ransomwares* et d'attaques contre les industries augmente le potentiel de dommages réels aux infrastructures critiques, brouillant la frontière entre l'hacktivisme et le cyberterrorisme - un fait qui peut finalement conduire à des réponses plus énergiques de la part des États victimes et au potentiel d'escalade du conflit.

Une autre évolution pertinente est le développement remarquable d'alliances émergentes entre les causes hacktivistes qui transcendent le théâtre des opérations au-delà de l'Ukraine et impliquent des pays tiers. Un exemple est la récente alliance entre les hacktivistes pro-russes et pro-palestiniens, qui réunit des causes géopolitiques apparemment distinctes sous un récit commun d'attaque de l'Occident.

⁴ Système centralisé permettant de surveiller, de contrôler et de collecter des données en temps réel à partir de processus et d'appareils.

Les tensions mondiales de 2024 (y compris la guerre de Gaza) ont créé un étrange front uni d'hacktivistes. Des groupes russes (en particulier *NoName057(16)*) ont commencé à coordonner leurs opérations avec des collectifs liés au Moyen-Orient (tels que *Mr. Hamza* ou *Anonymous Guys*), et ont synchronisé leurs attaques sous la bannière de l'union de la "*Sainte Ligue*" contre des pays qu'ils percevaient comme des adversaires communs, tels que la France.

Ce type d'alliance est bien connu en Espagne, et notamment par la Guardia Civil, puisqu'en juillet 2024, l'institution a été la cible directe d'une campagne de cyberattaque conjointe, "*#FuckGuardiaCivil*", qui répondait à une initiative promue par le groupe *NoName057(16)*, pour "se venger des autorités espagnoles" qui avaient arrêté trois personnes à Manacor (Majorque), Huelva et Séville, soupçonnées d'avoir participé à des cyberattaques contre des entités publiques et des entreprises stratégiques en Espagne et dans d'autres pays de l'OTAN.

En effet, en avril 2025, une nouvelle alliance était déjà enregistrée, comprenant les groupes *Keymous+*, *Mr Hamza*, *Alixsec* et *NoName057(16)*, pour attaquer la Pologne, l'Allemagne, la France, l'Italie et l'Espagne sous le slogan "*Operation Hack For Humanity V2 !*"

Rien qu'en Espagne, le premier jour de la campagne "*Operation Hack For Humanity V2 !*", plus de 30 attaques contre des sites web d'entreprises et de gouvernements ont été enregistrées, *M. Hamza*, *NoName057(16)*, *TwoNet* et *Keymous+* étant les groupes les plus actifs dans l'attaque.

La fréquence à laquelle cette convergence s'est produite ces derniers mois montre que le phénomène devient de plus en plus international et interconnecté. Les alliances entre groupes hacktivistes se renforcent mutuellement, dépassant les frontières du conflit russo-ukrainien dans un seul but : étendre leurs actions à l'ennemi commun occidental.

Le fait que des pays de l'OTAN tels que la France, l'Italie et l'Espagne puissent devenir la cible de *pirates informatiques* patriotes russes pourrait conduire à une escalade du conflit, en particulier si l'une de leurs attaques devait gravement endommager des infrastructures critiques, la cyberguerre de basse intensité pourrait susciter une réponse plus forte que d'habitude.

5. CONCLUSIONS

L'analyse de l'hacktivisme et de ses relations avec les États montre que ce phénomène a évolué de la protestation numérique à l'instrumentalisation étatique avec des implications géopolitiques et stratégiques. La frontière entre l'activisme, la cybercriminalité et les opérations étatiques est de plus en plus floue, en particulier dans les conflits tels que la guerre en Ukraine, où nous avons observé une instrumentalisation croissante des groupes hacktivistes par les forces gouvernementales dans la défense de leurs intérêts nationaux.

En effet, le conflit entre la Russie et l'Ukraine a marqué un tournant dans l'utilisation du cyberspace comme champ de bataille, où des acteurs étatiques et non étatiques se sont activement engagés dans des attaques par déni de service (DDoS), le cyberespionnage et le sabotage d'infrastructures critiques.

Cette étude, développée à travers l'étude des cas les plus importants sur la scène internationale, nous a permis d'établir une distinction entre les *hackers* civiques et les *hackers* patriotiques. Alors que les premiers embrassent des causes nihilistes ou socialement conflictuelles, les seconds sont utilisés par les États comme un outil clandestin dans les conflits internationaux, ce qui entraîne une externalisation des capacités cybernétiques gouvernementales et offre une série d'avantages stratégiques : déni plausible de responsabilité, prolongation des situations de tension ou réduction des coûts politiques et économiques.

En résumé, nous pourrions dire que les États ont appris à exploiter l'hacktivisme comme une arme supplémentaire, soit en se faisant passer pour des hacktivistes afin de désinformer ou d'exfiltrer des données, soit en encourageant leurs sympathisants à lancer des cyberattaques de masse contre leur ennemi.

Toutefois, cette instrumentalisation pose de sérieux problèmes au niveau stratégique. La sophistication progressive des attaques, qui sont passées du vandalisme numérique à des opérations plus avancées contre des infrastructures critiques, ne fait qu'accroître sérieusement les possibilités de représailles de la part des États touchés et le risque potentiel d'escalade dans les conflits asymétriques.

En outre, la convergence entre les APT et les hacktivistes remet en question les normes internationales existantes, car les attaques perpétrées par des acteurs *mandataires* brouillent la responsabilité des États et rendent difficile la mise en œuvre de la dissuasion ou de représailles directes. D'autant plus que les collectifs d'hacktivistes semblent évoluer vers un nouveau paysage d'alliances capables de rassembler des groupes d'hacktivistes aux agendas géopolitiques divers pour attaquer les pays occidentaux.

La cybersécurité des États doit s'adapter à une nouvelle réalité dans laquelle les groupes hacktivistes jouent un rôle clé dans la projection du pouvoir de l'État. Les démocraties occidentales, traditionnellement plus réticentes à utiliser de telles tactiques, sont confrontées à un dilemme : comment réagir efficacement sans compromettre leurs valeurs ?

La tendance actuelle montre non seulement une évolution claire de l'hacktivisme vers un lien croissant avec les intérêts du gouvernement qui le soutient, mais renforce également l'idée que le cyberspace continuera à prendre de l'importance dans les conflits futurs. Des cas tels que la Russie, où des groupes comme *Killnet* ou *NoName057(16)* ont revendiqué des cyber-opérations coïncidant avec les intérêts géopolitiques du Kremlin - en particulier pendant la guerre en Ukraine -, ou l'Iran, avec des groupes comme *Tapandegan*, dont la rhétorique oppositionnelle n'empêche pas les soupçons de coordination indirecte avec les agendas de l'État, illustrent cette dérive et renforcent l'idée que le cyberspace continuera à prendre de l'importance dans les conflits à venir, illustrent cette dérive, et démontrent un brouillage progressif entre acteurs non étatiques et étatiques dans la sphère numérique, où l'hacktivisme n'est plus exclusivement une forme de dissidence citoyenne mais est devenu, dans certains contextes, un outil informel de projection du pouvoir étatique.

6. RÉFÉRENCES BIBLIOGRAPHIQUES

- Antoniuk, D. (2024). *Cybervolk : Hacktivists from India and Russia collaborate on ransomware attacks (Cybervolk : des hacktivistes indiens et russes collaborent à des attaques par ransomware)*. The Record. <https://therecord.media/cybervolk-india-hacktivists-russia-ransomware>
- Antoniuk, D. (2024). *Cybervolk : Hacktivists from India and Russia collaborate on ransomware attacks (Cybervolk : des hacktivistes indiens et russes collaborent à des attaques par ransomware)*. The Record. <https://therecord.media/cybervolk-india-hacktivists-russia-ransomware>
- Auty, C. (2004). L'hactivisme politique : outil de l'opprimé ou fléau du cyberspace ? *Aslib Proceedings*, 56(4), 212-221.
- Bartlett, J. (2015). *The dark net : Inside the digital underworld*. Melville House.
- CFR (2012). *Attaques par déni de service contre les banques américaines en 2012-2013*. Conseil des relations étrangères (CFR). <https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013>
- Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy : The many faces of Anonymous*. Verso Books.
- Cyberknow (2025). *Guerre entre la Russie et l'Ukraine : le point sur les hacktivistes*. <https://cyberknow.substack.com/p/russia-ukraine-war-hackivist-update>
- CyberZaintza (2021). *Groupe APT*. <https://www.ciberseguridad.eus/ciberglosario/grupo-apt>
- Dahan, M. (2013). Hacking for the homeland : Patriotic hackers versus hacktivists. *Conférence internationale sur la guerre de l'information et la sécurité*, 51-VII. Academic Conferences International Limited. <https://search.proquest.com/docview/1549245919>
- Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism : The internet as a tool for influencing foreign policy. Dans J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars : The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.
- DOJ (2018). *Un grand jury inculpe 12 officiers de renseignement russes pour des délits de piratage liés à l'élection de 2016*. Département de la justice des États-Unis. <https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>
- Expósito Guisado, J. (2023). *Cyberproxies : APTs as a future risk factor (Les cyberproxies : les APTs comme facteur de risque futur)*. Institut espagnol d'études stratégiques (IEEE). *IEEE Bulletin*, (32), 815-831.

- FBI (2014). *Mise à jour de l'enquête sur Sony*. Federal Bureau of Investigation (FBI), Washington, D.C. <https://www.fbi.gov/news/press-releases/update-on-sony-investigation>
- Fox, A. C. (2019). *Conflict and the need for a theory of proxy warfare (Le conflit et la nécessité d'une théorie de la guerre par procuration)*. *Journal of Strategic Security*, 12(1), 44-71, JSTOR. www.jstor.org/stable/26623077
- Goode, L. (2015). Anonymous et l'éthique politique de l'hactivisme. *Popular Communication*, 13(1), 74-86. <https://doi.org/10.1080/15405702.2014.978000>
- Green, K. (2016). People's war in cyberspace : Using China's civilian economy in the information domain. *Military Cyber Affairs*, 2(1). <https://doi.org/10.5038/2378-0789.2.1.1022>
- Healey, J. et Grinberg, A. (2022). *Patriotic hacking : No exception*. Lawfare. <https://www.lawfaremedia.org/article/patriotic-hacking-no-exception>
- Hern, A. (2017). Un contractant de la NSA a divulgué des outils de piratage américains par erreur, selon Kaspersky. *The Guardian*. <https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office>
- Hunsinger, J. et Schrock, A. (2016). La démocratisation du piratage et de la fabrication. *New Media & Society*, 18(4), 535-538. <https://doi.org/10.1177/1461444816629466>
- Johnson, P. et Robinson, P. (2014). Civic hackathons : Innovation, procurement, or civic engagement ? *Review of Policy Research*, 31(4), 349-357. <https://doi.org/10.1111/ropr.12074>
- Jordan, T. (2002). *Activisme ! Action directe, hactivisme et avenir de la société*. Reaktion Books.
- Jordan, T. et Taylor, P. A. (2004). *Hactivism and cyberwars : Rebels with a cause ?* Psychology Press.
- Mandiant (2022). *L'ascension du GRU : les sous-fifres de Telegram*. <https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions>
- Marín, F. (2023). *L'hactivisme au service de l'État : les cyberproxies en Ukraine*. Opinion Paper. Institut espagnol d'études stratégiques (IEEE).
- Maurer, T. (2018). *Cyber Mercenaires : l'État, les hackers et le pouvoir*. Cambridge University Press.

- Muncaster, P. (2024). *Hacktivisme : évolution des menaces pour les organisations*. WeLiveSecurity. <https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones>
- Olson, P. (2012). *5 choses que chaque organisation peut apprendre des Anonymous*. Forbes. <http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/>
- OPTIV (2023). *Mise à jour Russie/Ukraine - décembre 2023*. <https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023>
- Popovic, M. (2015). Fragile proxies : Explaining rebel defection against their state sponsors. *Terrorisme et violence politique*. <https://doi.org/10.1080/09546553.2015.1092437>
- Rondeaux, C. et Sterman, D. (2019). *Twenty-first century proxy warfare : Confronting strategic innovation in a multipolar world since the 2011 NATO intervention*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf
- Sauter, M. (2013). "LOIC will tear us apart" : l'impact de la conception des outils et des représentations médiatiques sur le succès des attaques DDOS des activistes. *American Behavioral Scientist*, 57(7), 983-1007. <https://doi.org/10.1177/000276>
- Schrock, A. R. (2016). Civic hacking as data activism and advocacy : A history from publicity to open government data. *New Media & Society*, 18(4), 581-599. <https://doi.org/10.1177/1461444816629469>
- Torres Soriano, M. (2017). Proxy wars in cyberspace (Guerres par procuration dans le cyberespace). *Revista del Instituto Español de Estudios Estratégicos*, (9), 15-36.
- (2018). L'hactivisme comme stratégie de communication, des Anonymous au cybercalifat. *Cuadernos de Estrategia*, (197), 197-224.
- Van Der Walt (2025). *Réflexion sur trois années de cyberguerre en Ukraine*. ComputerWeekly. <https://www.computerweekly.com/opinion/Reflecting-on-three-years-of-cyber-warfare-in-Ukraine>
- Vegh, S. (2005). *The media's portrayal of hacking, hackers, and hacktivism before and after September 11. First Monday*. <http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126>



Article de recherche

PROTECTION INTERNATIONALE ET SOVERAINETÉ : L'ÉQUILIBRE COMPLEXE ENTRE LES DROITS INDIVIDUELS ET LA SÉCURITÉ NATIONALE

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

Alejandro Gómez García
Capitaine de la Guardia Civil
Master en gestion de la sécurité opérationnelle
Licence en droit
alejandrogomezg@guardiacivil.es
ORCID: <https://orcid.org/0000-0003-0162-4213>

Reçu le 31/03/2025
Accepté le 28/04/2025
Publié le 27/ 06/2025

Citation recommandée : Gómez, A. (2025). Protection internationale et souveraineté : l'équilibre compliqué entre les droits individuels et la sécurité nationale. *Revista Logos Guardia Civil*, 3(2), p.p. 123-146.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

PROTECTION INTERNATIONALE ET SOUVERAINETÉ : L'ÉQUILIBRE COMPLEXE ENTRE LES DROITS INDIVIDUELS ET LA SÉCURITÉ NATIONALE

Résumé: ANALYSE THÉORIQUE ET MÉTHODOLOGIQUE : ÉTATS, FRONTIÈRES ET PROTECTION INTERNATIONALE. 2.1 Carte conceptuelle de l'environnement frontalier. 2.2. 2.2 Migration et asile 3. ANALYSE JURIDIQUE : POSITIONS OPPOSÉES ET RÉPONSE DES TRIBUNAUX. 3.1. *L'affaire Hirsi Jamaa c. Italie* : la genèse d'une doctrine. 3.2. *N. D. et N. T. c. Espagne* : les limites de la protection. 3.3 Analyse comparative : la compatibilité d'une doctrine jurisprudentielle disparate. 4. CONCLUSIONS.

Résumé : L'objectif de cet article est d'analyser le statut juridique actuel de certains des concepts les plus pertinents dans le domaine de la protection des frontières nationales, ainsi que leur contexte sociopolitique et leur portée juridique, dans le but ultime de soutenir et de promouvoir le développement d'un débat doctrinal aussi brûlant dans ses positions que complexe dans son contexte : assurer un équilibre adéquat entre la garantie des droits fondamentaux des individus traversant les frontières européennes et l'exercice des pouvoirs souverains inhérents aux États. Ainsi, dans un premier temps, un examen détaillé des notions les plus importantes dans le domaine de la sécurité des frontières sera effectué, établissant le champ d'étude d'un point de vue scientifique. Immédiatement après, d'un point de vue juridique, nous étudierons les implications des déclarations les plus importantes faites par les organes judiciaires (fondamentalement internationaux) qui ont traité de la question, ainsi que la position de la doctrine et de la pratique internationales. Enfin, à la lumière des analyses présentées, nous proposerons une série de conclusions cohérentes avec les résultats obtenus.

Resumen: En el presente artículo se pretende analizar el estatus jurídico que ostentan, en la actualidad, algunos de los conceptos más relevantes dentro del ámbito de la protección de las fronteras nacionales, así como su contexto sociopolítico y su alcance jurídico, con el fin último de fundamentar e impulsar el desarrollo de un debate doctrinal tan candente en sus posturas como complejo en su contexto: Asegurar un adecuado balance entre la garantía de los Derechos Fundamentales de los individuos que transitan por las fronteras europeas y el ejercicio de las potestades soberanas consustanciales a los Estados. Así, en primer lugar, se realizará un examen pormenorizado de las nociones más importantes en el ámbito de la seguridad fronteriza, fijando el campo de estudio desde un punto de vista científico. Inmediatamente a continuación se estudiarán, desde una perspectiva jurídica, las implicaciones que han tenido los pronunciamientos más importantes efectuados por los órganos judiciales (fundamentalmente internacionales) que han entendido de la materia, así como la posición de la doctrina y la práctica internacional. Y finalmente, a la luz de los análisis expuestos, se ofrecerá una serie de conclusiones coherentes con los hallazgos efectuados.

Mots-clés : Droit international, asile, souveraineté, frontières, immigration.

Palabras clave: Derecho Internacional, Asilo, Soberanía, Fronteras, Inmigración.

ABBREVIATIONS

AN : Audiencia Nacional

ANP : Autorité nationale palestinienne

CFREU : Charte des droits fondamentaux de l'Union européenne

CEDH : Convention européenne des droits de l'homme

OMI : *Organisation maritime internationale - Organisation maritime internationale*

SAR : *Recherche et sauvetage - Recherche et sauvetage*

SOLAS : *Sécurité de la vie en mer - Sécurité de la vie en mer*

CEDH : Cour européenne des droits de l'homme

CIJ : Cour internationale de justice

CPA : Cour permanente d'arbitrage

CPJI : Cour permanente de justice internationale

UE : Union européenne

1. INTRODUCTION

À la suite de l'arrêt de la Cour européenne des droits de l'homme (ci-après CEDH), troisième section, du 3 octobre 2017, par lequel l'État espagnol a été condamné, dans le cadre de la pratique du "rejet à la frontière", pour violation de l'article 13 de la Convention européenne des droits de l'homme (ci-après CEDH) et de l'article 4 de son Protocole n° 4, prévoyant le versement d'une indemnité aux requérants N. D. (ressortissant malien) et N.T. (ressortissant ivoirien) à hauteur de 5 000 euros chacun ; de nombreuses voix se sont élevées pour demander un changement de cap complet dans la politique migratoire développée par le Royaume d'Espagne et, par extension, dans la politique migratoire européenne. En effet, la nouvelle a fait les gros titres de la presse¹, mais aussi de la presse écrite, avec des déclarations fortes d'organisations non gouvernementales² et même d'entités de droit public³, dans un pays qui n'a pas l'habitude de suivre la chronique judiciaire avec autant de détails, et encore moins au niveau international.

Et la situation n'était pas à prendre à la légère. La préoccupation croissante concernant le contexte migratoire dans l'Union européenne (ci-après UE) avait donné lieu, au fil des ans, à l'émergence de certains débats qui, jusqu'alors, étaient restés en dehors de la dynamique politique, qui acceptaient comme quelque chose de presque anecdotique l'augmentation soutenue du nombre de ressortissants de pays tiers résidant dans l'Union, dont le nombre avait augmenté de plus de 10 % au cours des trois années précédant la prise de position susmentionnée⁴. Bien entendu, la montée de ce débat a également été alimentée par ce que l'on appelle la "crise des réfugiés" de 2015, au cours de laquelle des centaines de milliers de personnes déplacées du Moyen-Orient (principalement des Syriens) ont pénétré sur le territoire européen en raison de l'instabilité et de la guerre qui sévissent dans la région. Et cela ne contribuerait certainement pas à apaiser les tensions dans la société européenne si certaines des personnes impliquées dans divers actes terroristes qui ont eu lieu au cours de ces années (par exemple, les attentats d'Ansbach et de Berlin en 2016 ou, bien sûr, les attentats de Paris en 2015) étaient ensuite identifiées comme des réfugiés ou des immigrants illégaux, venant de Syrie via la route de la Méditerranée orientale.

Mais, comme si cela ne suffisait pas, l'avenir nous réservait une nouvelle surprise de taille qui allait une fois de plus bouleverser le scénario de la politique migratoire européenne. Dans un événement sans précédent, la même CEDH qui avait renversé la doctrine espagnole sur les rejets aux frontières allait revenir sur sa décision en première instance et, dans un arrêt de la Grande Chambre du 13 février 2020, allait déclarer, à une majorité de 16 contre 1, la pleine légalité des rejets aux frontières. Puis vint la pandémie. Et avec elle, la réactivation de la route migratoire atlantique vers les îles Canaries, ainsi qu'un nouvel essor des mouvements migratoires vers l'UE en général, qui passeront de

¹ RTVE (3 octobre 2017), *La Cour européenne des droits de l'homme condamne l'Espagne pour deux "retours chauds" à Melilla*, <https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml>.

² Commission espagnole d'aide aux réfugiés (3 octobre 2017), *La Cour européenne des droits de l'homme condamne l'Espagne pour deux "retours chauds"*, <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>.

³ Consejo General de la Abogacía Española (3 octobre 2017), *La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH*, <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>.

⁴ Données Eurostat, https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en.

125 226 entrées illégales détectées en 2020 (Frontex, 2021, p. 14) à 380 227 en 2023 (Frontex, 2024, p. 1). Aujourd'hui, l'immigration occupe une place prépondérante parmi les principales préoccupations des citoyens du continent. Ainsi, le dernier "Eurobaromètre", publié en novembre 2024, place l'immigration au deuxième rang des domaines d'action de l'UE selon les Européens, une position soutenue par 29% des répondants (Commission européenne, 2024, p. 14), derrière la sécurité et la défense.

Cependant, bien que la Commission européenne n'hésite pas à répondre à ces préoccupations en soulignant à plusieurs reprises les " progrès " réalisés en matière de " gestion des frontières " (Commission européenne, 2022, p. 5), le fait est que lorsque le facteur de la sauvegarde des droits fondamentaux est introduit dans l'équation, la situation devient plus compliquée. En effet, les politiques visant à renforcer le contrôle des frontières, développées sur la base des objectifs de renforcement du système sur lequel repose la sécurité nationale et de garantie de la souveraineté des États, impliquent des mesures visant à entraver l'immigration illégale qui, par leur nature même, affectent les droits de la population concernée. Et, conformément aux règles de base de l'État de droit, si cet impact n'est pas adapté, cohérent et proportionnel aux fins légitimes poursuivies, il peut représenter une intrusion illégale dans le noyau le plus essentiel des droits fondamentaux, en particulier lorsqu'ils conditionnent des domaines clés tels que le droit d'asile. Cet article de recherche vise à analyser cet équilibre délicat, en révélant les points de friction entre les deux réalités conflictuelles grâce à un examen détaillé de la jurisprudence nationale et internationale ; ainsi qu'à clarifier, dans la mesure du possible, jusqu'où peut aller la légalité des actions des gardes civils en leur qualité de gardes-frontières.

2. ANALYSE THÉORIQUE ET MÉTHODOLOGIQUE : ÉTATS, FRONTIÈRES ET PROTECTION INTERNATIONALE

2.1. CARTE CONCEPTUELLE DE L'ENVIRONNEMENT FRONTALIER

2.1.1 Le concept de frontière

Le terme "frontière" a presque autant de significations qu'il y a de branches de la science qui ont envisagé l'étude de tout concept dérivé de la notion intuitive de "frontière". Des mathématiques aux sciences politiques, des relations internationales au droit. Sanz Do-naire (2023, p. 254) précise que le terme en question vient du terme latin classique *frons*, dont le sens renverrait à "front" ou "façade", et offrirait déjà une idée du contexte antagoniste ou distinctif dans lequel il se développerait depuis sa formulation, fortement liée à la sphère militaire, à la protection contre l'étranger, l'extérieur. En effet, les frontières sont liées au conflit et à la confrontation depuis le traité de Mesilim, considéré comme le " plus ancien traité enregistré " (Doebbler, 2018, p. 374-375), qui n'était rien d'autre qu'un accord réglant la reconnaissance des frontières entre plusieurs royaumes mésopotamiens vers 2500 avant notre ère. Curzon (1907) s'est également exprimé en ce sens à l'aube de l'étude scientifique des relations internationales, en affirmant que les tensions frontalières ont été le facteur le plus important des conflits entre États (p. 4).

Quoi qu'il en soit, c'est sur ces antécédents étymologiques que se fondent les conceptions actuelles de la frontière, parmi lesquelles le Dictionnaire d'espagnol juridique se distingue par sa puissance discursive, qui affirme ce qui suit :

"Frontière (droit international public) : *Ligne marquant la limite extérieure du territoire d'un Etat, entendu comme l'espace terrestre, maritime et aérien sur lequel il exerce sa souveraineté, ce qui permet de parler de frontières terrestres, maritimes et aériennes en fonction de la nature physique de l'espace délimité.*

2.1.2 Frontières et souveraineté

Selon la thèse de Lacan (1966), la compréhension des concepts repose sur la compréhension des relations qu'ils développent par rapport aux notions antérieures qui en constituent le sens, au moyen d'une concaténation de références dans ce que le psychanalyste français connaissait sous le nom de " chaînes de signifiants " (pp. 501-502). En ce sens, et compte tenu de la définition énoncée dans la section précédente, il semble évident que l'on ne peut parvenir à une compréhension satisfaisante de la réalité étudiée sans étudier au préalable l'autre concept technique qui y est en jeu : celui de souveraineté.

Ce concept a fait couler beaucoup d'encre. Depuis la première approche de Jean Bodin au XVI^e siècle, dans laquelle les composantes nationales, territoriales et théologiques étaient intrinsèquement liées, la notion de souveraineté est liée à l'existence d'un lien qui dépasse la simple extension physique et sociale dans laquelle s'exerce le pouvoir, et qui transcende en quelque sorte le territoire stricto sensu. C'est peut-être pour cette raison qu'il n'y a pas beaucoup de sources écrites de droit international qui offrent une définition cristalline et universelle de la souveraineté. L'un des rares textes qui peuvent nous donner quelques indices à cet égard est la Convention de Montevideo de 1933 sur les droits et les devoirs des États. Ce traité propose ce qui, dans la pratique, a fini par devenir une définition de la souveraineté, en établissant, à l'article 1, les conditions de base pour qu'une entité étatique soit considérée comme un sujet de droit international :

1. Population permanente.
2. Territoire déterminé.
3. Le gouvernement.
4. Capacité à nouer des relations avec d'autres États.

Il convient de noter que, bien que ce traité ne soit formellement applicable qu'au très petit nombre d'États qui l'ont signé (il a été convenu lors de la septième Conférence internationale des États américains, le prédécesseur direct de l'Organisation des États américains), il " a reçu une adhésion générale d'un point de vue doctrinal " (Infante Caffi, 2016, p. 66), ses postulats s'étendant progressivement - soit par référence directe, soit par référence à une coutume internationale fondée sur eux - à une généralité d'acteurs internationaux, y compris l'Union européenne elle-même. 66), étendant progressivement ses postulats - soit par référence directe, soit par référence à une coutume internationale fondée sur eux - à une généralité d'acteurs internationaux, y compris l'Union européenne elle-même⁵.

⁵ Voir, par exemple, les conclusions du Conseil européen sur le processus de paix au Moyen-Orient du 20 juillet 2015 ou la résolution du Parlement européen sur le rôle de l'UE dans le processus de paix au Moyen-Orient du 10 septembre 2015 ; qui promeuvent une voie vers la reconnaissance de la Palestine en tant qu'entité politique ("solution à deux États") sur la base d'une population permanente (mentionnée à plusieurs reprises comme "population palestinienne"), d'un territoire permanent (notant son attachement aux "frontières de 1967"), d'un gouvernement effectif (incarné par l'"Autorité palestinienne", ci-après ANP, qui est

De même, la jurisprudence internationale a progressivement défini le concept de souveraineté, étant entendu qu'en l'absence de titre objectif (par exemple, un traité de frontière signé et respecté par tous les États concernés), un État est considéré comme souverain sur un territoire lorsqu'il manifeste son intention de l'être par des moyens adaptés à cette fin en droit international (par exemple, une déclaration unilatérale) et, en même temps, lorsque cet État est capable d'exercer cette autorité de manière pratique, par le développement effectif de sa juridiction sur le territoire (arrêt de la Cour permanente de justice internationale du 19 avril 1955), une déclaration unilatérale) et, en même temps, lorsque cet État est en mesure d'exercer cette autorité d'une manière pratique, par le développement effectif de sa juridiction sur le territoire (arrêt de la Cour permanente de justice internationale du 5 avril 1933, pp. 45-27 in fine, 46-28 in limine ; arrêt de la Cour internationale de justice du 17 décembre 2002, par. 134, p. 182-61 ; sentence de la Cour permanente d'arbitrage du 9 octobre 1998, par. 239, p. 268 ; entre autres).

C'est sur la base de cette souveraineté que sera fondé le droit légitime des États à protéger leurs frontières, habituellement protégé par les règles traditionnelles du droit international coutumier et la référence à l'article 51 de la Charte des Nations unies ; et dans le cas européen, ce droit transcendera le niveau national, compte tenu de l'obligation internationale que l'accord de Schengen implique pour ses signataires.

2.2. MIGRATION ET ASILE

En revanche, lorsqu'il s'agit de concepts liés aux droits détenus par les individus dans la zone frontalière, il n'est pas rare que certains malentendus surgissent (par exemple, en ce qui concerne les notions d'"immigré" et de "réfugié"), d'où l'intérêt d'étudier brièvement mais rigoureusement un tel environnement juridique, notamment en ce qui concerne le contenu et l'étendue de la protection internationale.

2.2.1 Le droit d'asile et la protection subsidiaire

Le terme "asile" vient du grec *asylon*, un mot dont la traduction est proche de celle de "lieu inviolable". Dans sa conception initiale, il s'agit de la condition accordée au *hieron*, sorte d'espace spécial situé à l'intérieur des *téménos*, espaces consacrés aux dieux (Harris Díez, 2011, p. 70), qui échappaient à la juridiction de l'État, "et pouvaient ainsi devenir le refuge d'individus persécutés, d'esclaves en fuite ou d'hommes politiques" (Zaidman et Schmitt-Pantel, 2002, p. 45). C'est dans ce contexte que s'est formé le dogme chrétien de "l'asile dans le sacré", un statut d'immunité traditionnellement conféré aux lieux de culte afin de protéger les nécessiteux et de racheter les criminels repentis (Golmayo, 1866, pp. 88-89), d'où découlera plus tard le concept moderne de "droit d'asile".

Ce concept moderne du droit d'asile sera établi fondamentalement par la proclamation de deux textes : la Convention de Genève de 1951 relative au statut des réfugiés (ci-après la Convention de Genève), qui établit le concept de refuge ; et son Protocole de 1967, qui généralise cette protection, initialement créée pour un groupe très limité de bénéficiaires. La combinaison de ces deux textes permet d'aboutir à une définition unique qui reconnaît comme réfugié ou bénéficiaire de l'asile toute personne qui :

expressément citée) et d'une capacité à nouer des relations avec d'autres États (citant et reconnaissant les accords conclus avec l'ANP susmentionnée).

"...craignant avec raison d'être persécuté du fait de sa race, de sa religion, de sa nationalité, de son appartenance à un certain groupe social ou de ses opinions politiques, se trouve hors du pays dont il a la nationalité et ne peut ou, du fait de cette crainte, ne veut se réclamer de la protection de ce pays ; ou, se trouvant hors du pays dans lequel il avait sa résidence habituelle, ne peut ou, en raison de cette crainte, ne veut y retourner".

D'autre part, bien qu'il s'agisse de la définition générale, le fait est que les différents modèles de protection des droits fondamentaux existants ont développé toute une série de règles qui élargissent et clarifient le contenu de ce droit. Dans l'Union européenne, ce travail est réalisé par le biais de la directive 2011/95/UE, qui établit des aspects fondamentaux dans le processus d'obtention du statut de réfugié, tels que les critères d'évaluation des circonstances pouvant être considérées comme des persécutions, tout en introduisant dans le droit communautaire la "protection subsidiaire", une garantie qui préserve la situation juridique des ressortissants de pays tiers et des apatrides qui, "sans remplir les conditions d'obtention de l'asile, [...] il y a de sérieuses raisons de croire qu'ils se trouvent dans une situation de persécution", et qui, "ne remplissant pas les conditions d'obtention de l'asile, [...] il y a de sérieuses raisons de croire qu'ils se trouvent dans une situation de persécution". il y a des motifs sérieux de croire qu'elles courent un risque réel si elles retournent dans leur pays d'origine [...]" (art. 4). Cette protection subsidiaire - qui, avec le droit d'asile, forme ce que l'on appelle génériquement dans la terminologie de l'UE la "protection internationale" - vise à étendre l'indemnisation du statut de réfugié aux personnes qui risquent d'être condamnées à mort, soumises à la torture ou même de subir les conséquences d'un conflit militaire.

En tout état de cause, tous les règlements susmentionnés établissent explicitement l'inapplicabilité de cette protection à ceux qui peuvent être considérés comme des auteurs de crimes internationaux graves (criminels de guerre, génocides, etc.), des fugitifs de crimes de droit commun graves ou des personnes qui représentent un danger pour la sécurité du pays d'accueil.

2.2.2 Droits applicables aux bénéficiaires d'une protection internationale

Toute protection internationale accorde une série de droits minimaux à ses bénéficiaires, même si certains aspects accidentels de ceux-ci (délais, extension, etc.) peuvent varier légèrement selon que le statut accordé est celui de l'asile (plus protégé) ou de la protection subsidiaire (moins protégée). En outre, une partie importante de ces droits pourra être exercée non seulement par ceux qui ont été officiellement reconnus comme bénéficiaires d'un type quelconque de protection, mais les règlements européens reconnaissent également leur applicabilité aux simples demandeurs, tant que leur cas n'a pas été résolu⁶. En tout état de cause, il existe deux droits fondamentaux qui sont intrinsèquement liés à toute forme de protection internationale - y compris pour les demandeurs - et dont la nature sera décisive dans le conflit entre les droits individuels et la sécurité nationale : la protection judiciaire effective et le non-refoulement.

⁶ Par exemple, et conformément aux dispositions de la directive 2013/33/UE, le droit d'accès aux soins de santé (art. 19), aux aides publiques (art. 18) ou au marché du travail (art. 15).

2.2.2.1 Le droit à une protection judiciaire effective

Le droit à une protection judiciaire effective, entendu comme la garantie que les citoyens ont " accès à la juridiction, au traitement de la procédure, à la résolution [raisonnable] de l'affaire et à l'exécution de la sentence " (Carrasco Durán, 2020, p. 20), dans le cadre d'un système judiciaire équitable et impartial, n'est pas une garantie spécifique du droit d'asile, mais sa portée est universelle et, en tant que telle, elle est incluse dans la Constitution espagnole (art. 24) et dans la Constitution espagnole (art. 24). 20) dans le cadre d'un système judiciaire équitable et impartial, n'est pas une garantie spécifique du droit d'asile, mais sa portée est universelle et, en tant que telle, elle est incluse dans la Constitution espagnole (art. 24) et dans la Charte des droits fondamentaux de l'UE (art. 47), sous la référence permanente aux droits à un procès équitable (art. 6) et à un recours effectif (art. 13).

Cependant, son impact dans le domaine du droit d'asile a été notable, au point que la directive 2013/32/UE garantit (art. 46) l'accès au recours dans les procédures d'asile, en indiquant explicitement qu'il doit être entendu par un organe "judiciaire". Ainsi, l'une des allégations les plus récurrentes lors de la contestation des actions de l'État dans la zone frontalière a été l'absence alléguée ou la précarité de l'accès aux recours judiciaires. En ce sens, et dans la sphère européenne, la garantie juridictionnelle ultime d'une protection judiciaire efficace a été canalisée - avant l'épuisement des instances nationales - par le recours à la Cour européenne des droits de l'homme pour violation de l'article 13 de la CEDH⁷. Toutefois, la jurisprudence de cette Cour est claire : pour constater une violation de l'article 13, il faut d'abord qu'il y ait une allégation plausible de violation d'un autre des droits garantis par la Convention. Bien qu'il ne soit pas nécessaire qu'une telle violation ait effectivement eu lieu, il a été exigé qu'il y ait un tel *grief défendable* au titre de la Convention - CEDH (Grande Chambre) arrêt du 23 février 2012, *Hirsi Jamaa c. Italie*, §197, qui, à partir d'une première approximation plausible, permet ensuite de composer un récit fiable des faits, étant donné que la Convention vise à garantir des droits concrets et effectifs, et non théoriques ou illusoires - CEDH (Grande Chambre) Arrêt du 13 février 2020, *Affaire N. T. et N. D. c. Espagne*, §171-. Il est donc rare de constater des violations isolées de l'article 13 en l'absence de toute autre violation, même si, d'un point de vue doctrinal, cette possibilité existe et s'est effectivement produite - CEDH (Grande Chambre), arrêt du 8 juillet 2003, *Hatton et autres c. Royaume-Uni*. Dans le domaine du droit d'asile, cette relation s'est presque toujours traduite par un lien entre la violation et les violations de l'article 3 de la CEDH⁸ et de l'article 4 du protocole 4 de la CEDH.⁹

2.2.2.2 Droit de non-refoulement

Pour sa part, le droit au *non-refoulement* (consacré par l'article 33 de la Convention de Genève et généralement appelé *non-refoulement* dans la doctrine internationale) est un principe de base de la protection internationale qui implique la garantie que le bénéficiaire de la protection ne sera pas renvoyé dans son État d'origine ou dans tout autre État où il risque d'être persécuté, tant qu'il conserve son statut. Ce droit s'étend directement aux

⁷ "Toute personne dont les droits et libertés reconnus dans la présente convention ont été violés dispose d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles.

⁸ "Nul ne peut être soumis à la torture ni à des peines ou traitements inhumains ou dégradants.

⁹ "Les expulsions collectives d'étrangers sont interdites".

demandeurs pendant l'examen de leur dossier et, au niveau de l'UE, même à ceux dont la protection internationale n'a pas été officiellement accordée ou a été retirée (article 14, paragraphe 6, de la directive 2011/95/UE), dans la mesure où "ce sont les circonstances de fait d'une personne, [et] non la validation officielle de ces circonstances, qui donnent lieu au statut de réfugié au sens de la Convention" (Hathaway, 1995, 303-304). Et, en même temps, son respect est indépendant du fait que le demandeur se trouve ou non dans une situation légale dans le pays, un fait qui - bien qu'il ne soit pas explicitement mentionné dans les articles de la Convention - a été imposé par le biais du droit international coutumier et, dans le cas européen, a été établi par l'article 19 de la CDFUE et l'article 9 de la directive 2013/32/UE, étant approuvé par une jurisprudence répétée et pacifique à cet égard dans le cadre du système européen de protection des droits de l'homme¹⁰. Cela signifie que le droit au non-refoulement a été configuré comme faisant partie du noyau le plus essentiel des droits des réfugiés, dans la logique que sa violation systématique signifierait, en pratique, le vide du contenu de la protection internationale.

Il convient de noter que ce principe admet une exception : l'article 33.2 de la Convention de Genève garantit son inapplicabilité dans les cas où il existe des "raisons sérieuses" de considérer que le bénéficiaire ou le demandeur d'une protection internationale peut être considéré comme "un danger pour la sécurité du pays où il se trouve" (art. 33.2). Cette disposition, qui renforce les prérogatives des États dans le cadre de leur droit légitime à protéger leurs frontières, a été approuvée, avec certaines nuances¹¹, par la jurisprudence internationale. Un bon exemple en est l'arrêt de la CEDH (Grande Chambre) du 29 avril 1997, *L.H.R. c. France, dans l'affaire L.H.R. c. France. c. France*, dans lequel la Cour a approuvé l'expulsion d'un ressortissant colombien condamné pour trafic de drogue vers son pays d'origine, au motif que sa présence constituait une "menace grave pour l'ordre public", malgré les avertissements du requérant - partagés par la défunte Commission européenne des droits de l'homme, et même tièdement par la Cour elle-même - selon lesquels l'achèvement de son expulsion pourrait constituer un danger pour sa vie.

Enfin, dernier point notable, le développement du principe de non-refoulement a donné lieu, au fil du temps, à l'émergence d'un principe complémentaire qui a été généralement repris par les instruments juridiques internationaux les plus importants en la matière : l'interdiction des expulsions collectives d'étrangers. Ce précepte, que certains auteurs comme Kamto (2007) considèrent (non sans controverse) comme un "principe général du droit international" (p. 129), a été normativisé dans la CEDH (article 4 du Protocole 4) et dans la CFREU (article 19.1). Son contenu renvoie à l'approche selon laquelle toute expulsion d'étrangers doit être fondée sur des circonstances non arbitraires et nécessite donc une évaluation individuelle du contexte de chaque étranger.

¹⁰ Arrêts de la Cour européenne des droits de l'homme du 7 juillet 1989, *Soering c. Royaume-Uni* et, en particulier, du 15 novembre 1996, *Chahal c. Royaume-Uni*.

¹¹ Par exemple, la mise en œuvre de ce précepte au niveau européen ne doit pas conduire, par omission, à la violation de l'article 3 de la CEDH, qui proscriit la torture et les peines ou traitements inhumains ou dégradants ; Un élément qui, en revanche, est applicable à l'ensemble de la communauté internationale, ayant été considéré comme un argument de nature *jus cogens* (Arrêt du Tribunal pénal international pour l'ex-Yougoslavie du 22 février 2001, *Procureur c. Dragoljub Kunarac Radomir Kovac et Zoran Vukovic*, §466 ; ou Arrêt de la Cour internationale de justice du 20 juillet 2012, Questions relatives à l'obligation de poursuivre ou d'extrader, *Belgique c. Sénégal*, §99).

3. ANALYSE JURIDIQUE : POSITIONS CONTRADICTOIRES ET RÉPONSE DE LA COUR

3.1. *HIRSI JAMAA C. ITALIE* : LA GENÈSE D'UNE DOCTRINE

Sur la base de la législation susmentionnée, des décisions judiciaires successives ont progressivement défini le cadre réglementaire final qui, au moins pour le moment, régit l'équilibre complexe entre les pouvoirs légitimes de l'État et la sauvegarde des droits fondamentaux. À cet égard, un arrêt se distingue de tous les autres qui, en raison du délai dans lequel il a été rendu et de ses implications politiques ultérieures, a constitué une référence incontournable pour l'établissement des critères minimaux d'action à la frontière : l'arrêt (Grande Chambre) de la Cour européenne des droits de l'homme du 23 février 2012, *Hirsi Jamaa et al. c. Italie*.

Hirsi Jamaa est le nom d'un ressortissant somalien qui faisait partie d'un groupe d'environ deux cents immigrants clandestins débarqués dans le port de Tripoli entre le 6 et le 7 mai 2009. Ce débarquement a eu lieu directement à partir des trois navires de l'État italien (*Guardia di Finanza* et garde-côtes) qui avaient procédé, quelques heures auparavant, à l'interception et au sauvetage du groupe alors qu'il naviguait dans des embarcations précaires, à quelque 35 milles nautiques au sud de l'île de Lampedusa, dans la zone de recherche et de sauvetage maltaise (ci-après dénommée "SAR"). À la suite de ces événements, l'Italie a été poursuivie devant la CEDH, vingt-cinq parties s'étant jointes à l'affaire.

Cependant, ce qui était pertinent - pour sa nouveauté - dans l'affaire *Hirsi Jamaa* n'était pas tant l'application de l'article 3 de la CEDH dans le contexte d'un retour d'immigrants - une pratique déjà consolidée dans des arrêts tels que *Chahal c. Royaume-Uni* - mais plutôt que, pour la première fois, la Cour avait l'occasion de statuer sur le rejet d'immigrants interceptés dans l'environnement maritime en même temps qu'elle évaluait l'application extraterritoriale de la CEDH (Alarcón Velasco, 2015, p. 4). Et elle l'a fait en portant un coup retentissant à la thèse italienne, puisqu'elle a déclaré la violation des articles 3 et 13 de la CEDH, ainsi que de l'article 4 de son protocole numéro 4, dans tous les cas à l'unanimité.

Le raisonnement de base qui sous-tend la position de la Cour est le suivant :

1. D'une manière générale, la CEDH est applicable dans la mesure où, conformément aux articles 92 et 94 de la convention des Nations unies sur le droit de la mer, les navires sur lesquels les faits se sont produits sont soumis à la juridiction de l'État de leur pavillon, ce qui constitue un cas d'"exercice extraterritorial de la juridiction [...] susceptible d'engager la responsabilité de l'État".
2. En ce qui concerne l'article 3, l'élément déterminant a été l'impossibilité de considérer la Libye comme un "*lieu sûr*" pour le débarquement, la Cour estimant que non seulement la sécurité d'un point de vue maritime devait être prise en compte¹², mais aussi les questions relatives à la protection de leurs droits fondamentaux (violation du principe de non-refoulement).

¹² L'absence de risque dans les concepts relatifs à la sécurité en mer que l'on trouve dans les conventions internationales en la matière (en particulier dans les conventions SAR et SOLAS) se réfère principalement,

3. En ce qui concerne l'article 4 du Protocole 4, l'élément déterminant est l'absence d'individualisation de l'expulsion des immigrants, dans la mesure où ils n'ont pas été identifiés et où l'on n'a pas évalué si certains d'entre eux pouvaient avoir des circonstances personnelles pertinentes (violation de l'interdiction des expulsions collectives).

4. En ce qui concerne l'article 13, l'élément déterminant est l'impossibilité pour les immigrés d'avoir accès à un recours effectif contre la décision d'expulsion (violation du droit à une protection juridictionnelle effective), élément qui peut être apprécié au regard de la violation de l'article 3.

3.2. AFFAIRE *N.D. ET N.T. C. ESPAGNE* : LES LIMITES DE LA PROTECTION

Comme indiqué dans les sections précédentes, l'universalité du droit de demander une protection internationale n'implique pas que ce droit puisse être revendiqué ou exercé de manière illimitée. L'arrêt de la Cour européenne des droits de l'homme (Grande Chambre) du 13 février 2020, dans le cadre de l'affaire *N. D. et N. T. c. Espagne*, ne sera qu'un des meilleurs exemples de la manière dont les nations peuvent, de leur propre chef, mettre en place des systèmes efficaces de contrôle des frontières qui, à leur tour, respectent le droit international humanitaire, en luttant contre l'abus de droits dans une perspective de garantie.

Emulant l'analyse réalisée dans la section précédente concernant *Hirsi Jamaa*, la présente affaire concerne deux ressortissants étrangers, N. D. et N. T., qui, au sein d'un groupe d'environ 600 personnes, ont tenté de prendre d'assaut la clôture frontalière dans la ville de Melilla aux premières heures du 13 août 2014. Leur tentative a été déjouée grâce à l'action de la Guardia Civil et des forces de sécurité marocaines, les deux plaignants ont été escortés jusqu'à l'autre côté de la frontière, acte qui motivera le procès. Par la suite, les deux acteurs ont participé à deux nouveaux assauts contre la clôture, réussissant à pénétrer illégalement sur le territoire espagnol. Il convient de noter que l'un d'entre eux a ensuite demandé une protection internationale, qui lui a été refusée à toutes les étapes de la procédure.

A ce stade, l'intérêt de l'arrêt est double. D'une part, parce qu'il s'agit de l'approbation définitive de la pratique du "*rejet à la frontière*" (parfois appelée péjorativement "*retour à chaud*") : l'exécution d'un retour immédiat au Maroc de tout immigrant surpris en train d'essayer de franchir illégalement les éléments de confinement de la frontière. D'autre part, parce qu'il représente un contrepoint à *Hirsi Jamaa*, puisque tous deux marquent les limites de la légalité d'un point de vue différent : positif dans *N. D. et N. T.* (ce qui peut être fait), négatif dans *Hirsi Jamaa* (ce qui ne peut pas être fait), indiquant ainsi les deux limites entre lesquelles la législation frontalière doit se situer. Tout cela dans le contexte de l'existence, dans cette affaire, d'un jugement de première instance qui contredisait les arguments de l'Espagne, ce qui a donné lieu à un processus de justification plus détaillé de la part de la Grande Chambre en réponse aux demandes des plaignants, qui

par référence, à des aspects liés à la sécurité de la navigation ou à la sécurité opérationnelle (sécurité, sécurité en tant que protection contre le naufrage, contre la noyade, contre les risques inhérents à la cargaison du navire, etc.) Nonobstant ce qui précède, et par rapport au concept de "*lieu de sécurité*" existant dans la convention SAR de 1979, l'Organisation maritime internationale (ci-après OMI) elle-même a fini par intégrer des nuances qui complètent cette vision, aboutissant à des textes tels que l'annexe 34 de la résolution MSC.167(78) de l'OMI, *Lignes directrices sur le traitement des personnes sauvées en mer*, dans laquelle il est fait référence à des réglementations telles que la convention de Genève de 1951.

contestaient les actions des gardes-frontières pour violation de l'article 3 de la CEDH et de l'article 4 du Protocole 4 de la CEDH, ainsi que de l'article 13 de la CEDH en ce qui concerne les deux précédents.

Ainsi, le raisonnement de base qui sous-tend la position de la Cour est le suivant :

1. En ce qui concerne l'article 3, déjà au même stade d'admission (décision du 7 juillet 2015), la Cour rejette catégoriquement la recevabilité des arguments des requérants concernant la possibilité que le principe de non-refoulement (article 3 de la CEDH) ait été violé par le refus de renvoyer les immigrés au Maroc. Bien que le raisonnement juridique ne soit pas particulièrement détaillé, il met clairement en évidence l'absence de preuves permettant de considérer le Maroc comme un lieu dangereux à cette fin, et ne considère même pas - comme il l'a fait dans l'affaire *Hirsi Jamaa* - qu'il est nécessaire d'examiner la question de manière plus approfondie.

2. En ce qui concerne l'article 4 du Protocole 4, la position de la Cour est qu'une expulsion collective ne peut être considérée comme existant dans le contexte d'une action en vigueur déclenchée par le requérant lui-même, et qui provoque "une situation manifestement perturbatrice, difficile à maîtriser et mettant en danger la sécurité publique" (§201). Ceci est particulièrement pertinent si l'on tient compte du fait que, dans le jugement de la juridiction inférieure, la Chambre avait directement établi - sans même soulever une justification qui affecterait le fond de l'affaire - un parallélisme total entre cette affaire et *Hirsi Jamaa*, malgré le fait qu'il s'agisse de contextes totalement différents. Ainsi, la Cour prévoit qu'un tel "examen individualisé" pour surmonter l'obstacle conceptuel de l'expulsion collective doit être effectué en tenant compte "des circonstances particulières de l'expulsion et du "contexte général à l'époque des faits"" (§197), ce qui permet de simplifier ou d'omettre les procédures d'évaluation, surtout si ce contexte dépend largement "du propre comportement du requérant" (§200) et si l'Etat fournit "des procédures légales disponibles pour entrer [dans le pays]" (§208) et "garantit le droit de demander une protection [...] de manière réelle et effective" (§209). de manière réelle et effective" (§208).

3. En ce qui concerne l'article 13, la Cour précise qu'aucune violation du droit à une protection juridictionnelle effective ne peut être constatée, attribuant également l'absence de recours juridictionnel au "propre comportement des requérants qui ont tenté d'entrer à Melilla sans autorisation" (§242).

Enfin, une observation intéressante sur les motifs de l'arrêt est que, bien que la Cour rejette la thèse de l'Espagne concernant la limitation de la compétence sur la base de critères opérationnels - similaires à ceux soutenus par l'Italie dans l'affaire *Hirsi Jamaa* -, en déclarant que l'exercice effectif de l'autorité que l'Espagne, par l'intermédiaire de la Guardia Civil, exerce à partir du périmètre de la clôture extérieure vers l'intérieur (§§107-108), est indéniable, elle établit que le gouvernement espagnol ne peut être tenu responsable des circonstances qui se produisent en dehors de son territoire souverain. Le fait que le gouvernement espagnol exerce, par l'intermédiaire de la Guardia Civil, son activité à partir du périmètre de la clôture extérieure (§§107-108), établit que le gouvernement espagnol ne peut être tenu pour responsable des circonstances survenant en dehors de son territoire souverain, et en particulier de celles qui sont le fait d'agents d'un État tiers (§218).

3.3. ANALYSE COMPARATIVE : LA COMPATIBILITÉ D'UNE DOCTRINE JURISPRUDENTIELLE DISPARATE

Comme nous l'avons vu, tant l'affaire *Hirsi Jamaa et al. c. Italie* que l'affaire *N.D. et N.T. c. Espagne* représentent deux cas dans lesquels, pour des comportements a priori analogues (la remise à des autorités non européennes d'étrangers tentant d'entrer illégalement sur le territoire communautaire), la Cour européenne des droits de l'homme a rendu des arrêts différents. Et ceci est fondamentalement dû à l'existence dans les affaires *N.D. et N.T.* d'un fil conducteur qui a été dûment et opportunément revendiqué par l'Espagne dans le cadre des procédures suivies au cours du litige susmentionné, et qui articule, du début à la fin, l'arrêt : la doctrine du "comportement coupable".

Le corollaire de ce raisonnement est que l'Etat ne peut être tenu pour responsable du fait que les immigrés se soustraient aux procédures légales d'entrée sur le territoire, surtout s'ils "profitent délibérément de leur grand nombre et font usage de la force" (*N.D. et N.T. c. Espagne*, §201). Ainsi, pour que cette doctrine soit applicable, le comportement répréhensible imputable aux migrants doit générer une situation grave, résultant d'un comportement volontaire - c'est-à-dire conscient de son illégalité et de ses conséquences possibles - qui représente un danger objectif pour la sécurité publique, y compris celle des migrants eux-mêmes.

En effet, l'interprétation de la Cour transcende toutes les violations alléguées par les requérants, même celles qui sont (a priori) les plus éloignées de leur sphère d'action individuelle. Ainsi, en ce qui concerne l'interdiction des expulsions collectives d'étrangers (article 4 du protocole 4 de la CEDH), la Cour européenne des droits de l'homme va situer l'aspect différentiel dans les possibilités d'accès des immigrés aux procédures légales d'entrée sur le territoire européen. Ainsi, dans les affaires *N. D. et N. T.*, il est indiqué à plusieurs reprises que le droit espagnol offrait aux requérants diverses possibilités de traiter leur entrée en Espagne, ainsi que de demander l'asile¹³ (§212), mais que ces outils ont été refusés (comportement coupable) par les requérants (§231). Le même raisonnement s'applique en ce qui concerne le droit à une protection juridictionnelle effective (article 13 de la CEDH), les arguments utilisés par le Tribunal des garanties étant les mêmes (§242).

Ces prémisses étant posées, la question se pose inévitablement : la doctrine du comportement coupable pourrait-elle être utilisée, *mutatis mutandis*, pour les expulsions ayant lieu dans le domaine maritime ? Et, dans l'affirmative, que faudrait-il changer dans le cadre de l'action étatique pour y parvenir ? La réponse à ces questions n'est pas triviale. Après *N.D. et N.T.*, la Cour européenne des droits de l'homme a utilisé cette doctrine - qui n'était d'ailleurs pas tout à fait nouvelle au moment de sa formulation¹⁴ - à quelques

¹³ La possibilité offerte par la législation espagnole d'accéder à certaines procédures liées à l'asile dans les ambassades et les consulats (article 38 de la loi 12/2009, du 30 octobre, régissant le droit d'asile et la protection subsidiaire) est particulièrement remarquable, à la fois parce que la Cour a insisté à plusieurs reprises sur cette possibilité et parce qu'il ne s'agit pas d'une pratique courante dans d'autres États européens (l'Italie, par exemple, ne l'inclut pas dans son décret législatif du 19 novembre 2007, sur la reconnaissance de la protection internationale).

¹⁴ La Cour européenne des droits de l'homme avait déjà adopté une approche précurseur en 1996 dans l'affaire *John Murray c. Royaume-Uni* - arrêt (grande chambre) du 8 février 1996 - en refusant la protection à un homme condamné pour terrorisme qui alléguait que son silence avait été utilisé contre lui dans le cadre

reprises¹⁵, sans qu'aucune d'entre elles n'ait servi à entériner un refus maritime. Ce qui est certain, en revanche, c'est qu'il n'y a aucun passage dans *N.D. et N.T.* où la Cour affirme que sa doctrine n'est pas valable pour les expulsions d'immigrants interceptés en mer. Bien au contraire, l'arrêt souligne la nécessité d'une appréciation des "circonstances du cas d'espèce" (§201). De ce fait, et en vertu du principe *permissum videtur id omne quod non prohibetur*¹⁶, il semble logique de déduire que l'admissibilité d'un tel principe ne devrait dépendre que de la réalisation de ses présupposés intrinsèques, à savoir l'existence de véritables outils juridiques permettant d'accéder à l'État de destination et d'engager une procédure d'asile devant ses autorités ; ainsi que sur la constatation d'un comportement répréhensible de la part des immigrants qui, ignorant l'existence de ces outils juridiques, défient les mécanismes de contrôle aux frontières par le biais d'actions coercitives. En outre, ces deux conditions doivent être dûment invoquées par l'État dans le cadre de la procédure judiciaire, ce que l'Italie n'a pas fait dans l'affaire *Hirsi Jamaa*. Aucune de ces conditions préalables ne semble nécessairement invincible dans un scénario maritime typique dans lequel des centaines d'hommes d'origine et de parcours inconnus se mettent eux-mêmes, ainsi que leurs compagnons de voyage et les garde-frontières et garde-côtes européens, en danger manifeste en proposant un départ massif, planifié et coordonné d'embarcations à destination d'un territoire isolé, aux capacités d'accueil limitées, avec le risque d'effondrement qui en découle - comme Lampedusa. Tout ceci est soumis à la nécessité pour l'Etat côtier de disposer d'un déploiement diplomatique de taille adéquate avec des pouvoirs accordés dans le domaine de l'asile, ce qui lui permet de justifier la suffisance des mécanismes d'accès à l'asile. A cet égard, il convient également de mentionner la communauté que représente l'UE en termes de migration et d'asile, ce qui permettrait même de suggérer - bien qu'il soit peut-être nécessaire pour cela de progresser davantage dans le processus d'intégration européenne toujours lent - que l'existence de délégations diplomatiques d'autres pays de l'UE est un atout qui doit nécessairement être valorisé aux fins de l'évaluation adéquate des possibilités d'accès offertes par l'État plaignant, car il représente un renforcement inhérent des ressources propres de l'État.¹⁷

Et, dans la lignée de ce qui précède, il est également pertinent d'évoquer certaines déductions concernant le problème des limitations factuelles de l'État dans son action internationale. Bien que certains auteurs comme Sánchez Tomás (2018, p. 110) ou Martínez Escamilla (2021, p. 6-7) affirment que la territorialité est la perspective dominante en termes de détermination de la responsabilité internationale, la vérité est que tant la doctrine que la pratique internationales (déjà mentionnées au point 2.1.2 de ce texte) indiquent la nécessité d'un exercice pratique de la territorialité dans la détermination de la responsabilité internationale. La doctrine et la pratique internationales (déjà évoquées au

de sa procédure judiciaire. La Cour a jugé que c'était lui qui avait choisi de garder le silence alors qu'il était conscient des conséquences qu'un tel comportement pouvait entraîner, et que c'était donc lui qui s'était exposé à ce que son silence lui soit préjudiciable (§56).

¹⁵ Arrêt de la Cour européenne des droits de l'homme (troisième section) du 24 mars 2020, *Asady et autres c. Slovaquie*.

¹⁶ "Tout ce qui n'est pas interdit est considéré comme autorisé.

¹⁷ En effet, il semble évident de penser que, compte tenu de la préexistence d'un espace commun de liberté, de sécurité et de justice, dans le cadre duquel les frontières intérieures ont été abolies et qui a articulé des mécanismes de mise en œuvre d'une politique commune d'immigration et d'asile, un réseau constitué par l'ensemble de ses ambassades et consulats offre aux candidats à l'immigration une plate-forme d'accès beaucoup plus importante et diversifiée, avec un plus grand nombre de garanties procédurales, que celle offerte par un État séparé. Surtout si l'on tient compte de l'homogénéité qu'implique la législation européenne en matière de reconnaissance, de qualification, d'évaluation et de résolution des procédures d'asile, de séjour et de résidence légale, qui sont communes à tous ses États membres.

point 2.1.2 de ce texte) soulignent la nécessité d'un exercice concret de l'autorité sur ce territoire pour être considéré comme souverain, raison pour laquelle la Cour, dans son arrêt de Grande Chambre, modifie son arrêt de première instance en éliminant ou en adoucissant considérablement les mentions relatives à la prépondérance du tracé de la frontière par rapport au tracé effectif de la clôture (incluses au §53 de l'arrêt de première instance). Ainsi, comme nous l'avons déjà mentionné, le rejet de l'exemption du principe général d'attribution ne dépend pas de la territorialité du point où les actes ont lieu, mais du fait que l'action est menée par des agents de l'État signataire, indépendamment du lieu où l'action a lieu. Cela sera pertinent dans les cas (par exemple, les événements du 24 juin 2022 à Melilla) où l'Espagne a été tenue responsable d'actes commis par des fonctionnaires étrangers dans des zones qui, bien que formellement situées à l'intérieur de la frontière espagnole "historique", se trouvent en pratique au-delà de la clôture et ne font donc l'objet d'aucun contrôle effectif de la part de l'Espagne.

Enfin, il faut souligner le traitement différent que la Cour accorde à l'étude des possibles violations de l'article 3 CEDH (prévention de la torture et des traitements inhumains ou dégradants) dans *Hirsi Jamaa* et dans *N.D. et N.T.* Malgré le peu de justifications offertes par la décision de rejet de *N.D. et N.T.* à cet égard, il semble clair que la justification de cette différence réside, du moins pour l'essentiel, dans le pays d'expulsion. Une partie de la doctrine (Del Valle Gálvez, 2018, pp. 25-49 ; Freedman, 2024, 204-220) en est venue à avancer des thèses qui se rapprochent d'une remise en cause généralisée de ce qu'il est convenu d'appeler les "politiques d'externalisation des frontières", concept avec lequel il convient d'être très prudent. Tout d'abord, parce que ce terme péjoratif a été utilisé pour définir ce qui, dans la plupart des cas, n'est rien d'autre que des politiques de coopération policière internationale dans le domaine du contrôle des frontières, à travers lesquelles le renforcement des capacités est encouragé pour renforcer l'application de la loi dans les pays en développement. Ainsi, le terme même choisi semble plutôt malheureux, car il est difficile d'"externaliser" les tâches de contrôle des frontières et d'application de la loi, qui ne sont rien d'autre que des "obligations dérivées du droit conventionnel et coutumier", et donc l'objet du "*ius cogens*" (Soler García, 2017, p. 41). Et, d'autre part, parce que l'acceptation irrationnelle de positions tangentiellement contraires à ces politiques mettrait en péril non seulement l'application de mesures étatiques légitimes - l'expression de sa souveraineté en matière de sécurité nationale ou de politique migratoire - mais aussi les intérêts de la communauté internationale et la protection des droits de l'homme : après tout, le renforcement des capacités des États d'origine et de transit dans des domaines vitaux tels que la recherche et le sauvetage en mer de leurs propres compatriotes est également un élément essentiel de cette coopération. Il s'ensuit qu'une telle coopération ne peut en soi être en contradiction avec la CEDH.

Et c'est là qu'intervient le facteur véritablement différentiel de *Hirsi Jamaa* : la Libye. En ce sens, la situation de la Libye est certainement idiosyncratique. Il s'agit d'un État qui n'a pas signé la Convention de Genève et qui a été défini à plusieurs reprises par différents auteurs comme un "chaos", dans lequel "les migrants expulsés d'Europe ont souvent été abandonnés à un sort incertain" (Cole, 2012, p. 6). Et cela explique parfaitement les craintes exprimées par la Cour dans l'affaire *Hirsi Jamaa* (§136), sur la base de différents rapports intégrés dans l'affaire (HCR, Commission européenne, Conseil de l'Europe, Human Rights Watch, etc., voir §33-42). Cette situation n'est pas comparable à celle qui existe dans pratiquement tous les États avec lesquels l'Espagne a conclu des accords de rapatriement actifs et raisonnablement fonctionnels, principalement le Maroc et l'Algérie, des États qui font partie de la politique européenne de voisinage - qui exige,

conformément à l'article 8 du TUE, de partager les principes démocratiques de l'UE - et qui en ont grandement bénéficié, devenant des partenaires économiques et politiques privilégiés. Après tout, il existe une abondance de déclarations judiciaires¹⁸ qui approuvent explicitement leur statut de "pays tiers sûrs" (voir SAN 1441/2018 du 15 mars 2018 pour le cas du Maroc ou SAN 3838/2016 du 17 octobre 2016 pour le cas de l'Algérie). Et ce point est d'un grand intérêt non seulement aux fins du retour des migrants irréguliers dans leur pays d'origine, mais aussi par rapport à la possibilité (entérinée par l'article 3, paragraphe 3, du règlement 604/2013 relatif à la détermination de l'État membre responsable de l'examen d'une demande de protection internationale) d'orienter les demandeurs d'asile vers des centres situés dans des pays tiers sûrs au cours de l'examen de leur demande. Cette possibilité pourrait toutefois faire l'objet - compte tenu de sa complexité et des controverses prévisibles - d'un article à part entière, avec le débat doctrinal correspondant.

4. LES CONCLUSIONS

Pour conclure, nous ferons une brève synthèse de la doctrine examinée dans les chapitres précédents, en proposant quelques lignes directrices qui décrivent les résultats les plus intéressants dans la matière analysée.

Tout d'abord, la conclusion la plus générale et la plus évidente que l'on peut tirer de ce qui précède est que de nombreux phénomènes sociaux convergent dans l'environnement frontalier, ce qui génère un niveau élevé de contentieux en matière de protection des droits fondamentaux. Ces processus, qui découlent tous de la tension permanente entre les politiques de contrôle migratoire et les garanties individuelles, exigent un équilibre qui se règle souvent devant les tribunaux, mettant à l'épreuve les cadres juridiques nationaux et internationaux, ainsi qu'une série de concepts manipulés par la doctrine - frontière, souveraineté, territoire, asile, etc. Il est donc essentiel que les forces de sécurité qui fournissent leurs services aux frontières aient une connaissance suffisante de la législation qui les protège, afin d'exercer leurs fonctions de manière efficace, mais aussi dans le respect des droits des personnes qui traversent ces environnements.

D'autre part, il convient de noter que la majorité de ces procédures judiciaires sont fondées sur la violation de garanties très spécifiques, qui sont régulièrement répétées dans les déclarations des organes judiciaires chargés de leur poursuite. Il s'agit fondamentalement de la transgression des principes de non-refoulement et du droit à une protection juridictionnelle effective, doctrines dont la sauvegarde, dans le cadre européen, est consacrée par les articles 3 et 13 de la CEDH ; ainsi que de l'interdiction des expulsions collectives d'étrangers, protégée par l'article 4 du Protocole 4 de ladite Convention. Ces procédures judiciaires sont toutefois longues et très complexes, et leurs décisions sont souvent en conflit direct avec des décisions antérieures rendues par d'autres tribunaux, voire par les mêmes organes qui les ont rendues. Pour ces raisons, il est également essentiel que les organes chargés de la représentation et de la défense des États souverains aient

¹⁸ Pratiquement toutes ces prises de position proviennent des sphères nationales, étant donné que la Cour EDH évite les prises de position catégoriques sur la sécurité des États et privilégie l'analyse au cas par cas, tout comme les hautes juridictions espagnoles. En revanche, plusieurs pays européens ont établi des listes de pays tiers sûrs, incluant le Maroc dans certaines d'entre elles, comme c'est le cas, par exemple, aux Pays-Bas (Immigration and Naturalisation Service, 2018). Cette pratique gagne du terrain parmi les États européens et est conforme aux dispositions du Pacte sur les migrations et l'asile, qui a introduit ce concept dans le nouveau règlement sur les procédures d'asile (règlement (UE) 2024/1348), qui commencera à s'appliquer à partir du 12 juin 2026 (section V, art. 57 et suivants).

une connaissance approfondie du droit international et sachent rendre ces doctrines compatibles avec leur droit interne - en proposant même les modifications législatives nécessaires - afin d'assurer, en tant que garants de l'ordre juridique, que les décisions affectant leurs sphères de représentation soient conformes au droit et à la pratique internationaux.

Enfin, et dans la lignée de ce qui précède, on ne peut ignorer la mutabilité qui caractérise l'interprétation de l'ordre juridique international. Il ne s'agit pas d'une faiblesse du système en soi : les règles, surtout dans des environnements anarchiques comme celui-ci, sont en transformation permanente, et les opérateurs juridiques n'ont donc d'autre choix que d'adapter leurs positions aux réalités existantes, ce qui se fait depuis l'Antiquité, lorsqu'il existait des figures juridiques impensables dans le monde contemporain. En ce sens, un scénario aussi volatil que celui qui régit la géopolitique mondiale actuelle exige - dans le respect des consensus inhérents au maintien de la paix et de la sécurité internationales, parmi lesquels la prise en compte de la dignité de la personne en tant que source inaliénable des droits de l'homme - une certaine marge dans l'interprétation des normes qui régissent les obligations des États, une position qui n'est pas nouvelle dans la doctrine (Koskeniemi, 2004). De cette manière, le respect adéquat de ces normes est garanti, en respectant la volonté de leurs promoteurs tout en favorisant la coexistence, approfondissant ainsi le développement d'un environnement international prospère pour tous ses habitants.

RÉFÉRENCES BIBLIOGRAPHIQUES

- Alarcón Velasco, N. (2015), El abogado ante las normas de asilo : vigilancia de su aplicación, Consejo General de la Abogacía Española. Disponible en ligne : <https://www.abogacia.es/actualidad/noticias/el-abogado-ante-las-normas-de-asilo-vigilancia-de-su-aplicacion/>. [Consulté le : 31/03/2025].
- Carrasco Durán, M. (2020). La definición constitucional del derecho a la tutela judicial efectiva, in *Revista de derecho político*, núm. 107, 13-40.
- Cole, P. (2012), *Borderline Chaos ? Stabilizing Libya's Periphery*, Middle East, octobre 2012, Washington : Carnegie Endowment for International Peace.
- Commission espagnole d'aide aux réfugiés (3 octobre 2017), La Cour européenne des droits de l'homme condamne l'Espagne pour deux " retours chauds ". Disponible en ligne : <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>. [Consulté le 31/03/2025].
- Commission européenne (2022), Rapport sur l'état de Schengen 2022, Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2022) 301 final. Disponible en ligne : <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022DC0301>. [consulté le : 31/03/2025].
- Commission européenne (2024), Eurobaromètre standard. Les opinions des Européens sur les priorités de l'Union européenne, n° 102, Bruxelles : Office des publications de l'UE. Disponible en ligne : <https://europa.eu/eurobarometer/surveys/detail/3215>. [Consulté le 31/03/2025].
- Conseil de l'Union européenne (2015), Conclusions du Conseil sur le processus de paix au Moyen-Orient. Disponible en ligne : <https://www.consilium.europa.eu/en/press/press-releases/2015/07/20/fac-mepp-conclusions/pdf/>. [Consulté le 31/03/2025].
- Consejo General de la Abogacía Española (3 octobre 2017), La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH. Disponible en ligne : <https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/>. [Consulté le 31/03/2025].
- Curzon, G. (1907), *Frontiers*, Oxford : Clarendon Press.
- Del Valle Gálvez, A. (2019), La fragilidad de los derechos humanos en las fronteras exteriores europeas, y la externalización/ extraterritorialidad de los controles migratorios in *Anuario de los cursos de derechos humanos de Donostia-San Sebastián*, Vol. XVIII, Valencia : Tirant lo Blanch.
- Doebbler, C. (2018), *Dictionary of Public International Law*, Londres : Row-man & Littlefield.

- Eurostat (2025), Population au 1er janvier par groupe d'âge, sexe et nationalité. Disponible en ligne : https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en. [consulté le 31/03/2025].
- Freedman, J. (2024), *The violent externalisation of asylum* in *Research Handbook on Asylum and Refugee Policy*, pp. 204-220, Cheltenham : Edward Elgar Publishing.
- Frontex (2021), *Analyse des risques pour 2021*, Varsovie. Disponible en ligne : <https://www.frontex.europa.eu/publications/risk-analysis-for-2021-MmzGl0>. [Consulté le 31/03/2025].
- Frontex (2024), *Annual Brief 2023*, Varsovie. Disponible en ligne : <https://prd.frontex.europa.eu/document/annual-brief-2023/>. [Consulté le 31/03/2025].
- Golmayo, P. B. (1866), *Instituciones de Derecho Canónico*, Madrid : Imprenta de A. Peñuelas.
- Harris Díez, R. (2011), *El paisaje de los dioses : los santuarios griegos de la época clásica y su entorno natural*, in *AISTHESIS : Revista Chilena de Investigaciones Estéticas*, núm. 49, Santiago du Chili : Instituto de Estética de la Pontificia Universidad Católica de Chile.
- Hathaway, J. C. (2005), *The rights of refugees under International Law*, Cambridge : Cambridge University Press.
- Infante Caffi, M.T. (2016), *Las fronteras desde la perspectiva del Derecho Internacional*, in *Revista de Estudios Internacionales*, núm. 185, pp. 59-86, Santiago : Instituto de Estudios Internacionales de la Universidad de Chile. Disponible en ligne : https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692016000300004. [consulté le : 31/03/2025].
- Kamto, M. (2007), *Troisième rapport sur l'expulsion des étrangers*, Genève : Commission du droit international des Nations unies.
- Koskenniemi, M. (2004), *The Gentle Civilizer of Nations : The Rise and Fall of International Law 1870-1960*, Cambridge : Cambridge University Press.
- Lacan, J. (1966), *Écrits*, Paris : Éditions du Seuil.
- Martínez Escamilla, M. (2021), *Las "devoluciones en caliente" en el asunto N. D. y N.T. contra España* (Sentencia de la Gran Sala TEDH de 13 de febrero de 2020) in *Revista Española de Derecho Europeo*, Núm. 77.
- Haut-Commissariat aux droits de l'homme (2018), *Principes et directives recommandés concernant les droits de l'homme aux frontières internationales*, Genève : HCR. Disponible en ligne : <https://acnudh.org/principios-y-directrices-recomendados-sobre-los-derechos-humanos-en-las-fronteras-internacionales/>. [Accédé le 31/03/2025].

Parlement européen (2015), Résolution du Parlement européen sur le rôle de l'UE dans le processus de paix au Moyen-Orient. Disponible en ligne : https://www.europarl.europa.eu/doceo/document/TA-8-2015-0318_EN.html. [Consulté le : 31/03/2025].

Real Academia Española (2014), Diccionario de la lengua española (23e édition).

Real Academia Española, Diccionario panhispánico del español jurídico (DPEJ). Disponible en ligne : <https://dpej.rae.es/>. [Consulté le 31/03/2025].

RTVE (3 octobre 2017), La Cour européenne des droits de l'homme condamne l'Espagne pour deux " retours chauds " à Melilla. Disponible en ligne : <https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml>. [Consulté le : 31/03/2025].

Sánchez Tomás, J. M. (2018), Las "devoluciones en caliente" en el Tribunal Europeo de Derechos Humanos (STEDH, As. N.D. Y N.T. vs España, de 03.10.2017), in *Revista Española de Derecho Europeo*, núm 65, pp. 102-135.

Sanz Donaire, J. J. (2023). Del concepto de frontera, in *Boletín de la Real Sociedad Geográfica*, Número extraordinario 2023, pp. 253-262. <https://doi.org/10.22201/cei-ich.24485691e.2014.12.49710>.

Service de l'immigration et de la naturalisation (2018), Beoordeling veilige derde landen - Marokko, Informatiebericht SUA IB 2018/105. Disponible en línea: https://puc.overheid.nl/ind/doc/PUC_9890080000_1/1?solrID=PUC_9890080000_1_1&solrQ=morocco. [consulté le 31/03/2025].

Soler García, C. (2017), The European Border and Coast Guard : An advance on Frontex ? Una valoración provisional, in *Revista Electrónica de Estudios Internacionales*, núm. 34. Disponible en ligne : <https://www.reei.org/index.php/revista/num34/articulos/guardia-europea-fronteras-costas-avance-respecto-frontex-una-valoracion-provisional>. [consulté le : 31/03/2025].

Zaidman, L. B., Schmitt-Pantel, P. (2002), *La religión griega en la polis de la época clásica* (Díez Platas Trad.), Colmenar Viejo : Akal.

LÉGISLATION ET JURISPRUDENCE

Charte des Nations unies (1945), Conférence des Nations unies sur l'organisation internationale, signée à San Francisco le 26 juin 1945.

Convention sur les droits et les devoirs des États (1933), septième Conférence internationale américaine de Montevideo, Recueil des traités de la Société des Nations, volume 165, page 19.

Convention relative au statut des réfugiés (1951), Conférence de plénipotentiaires des Nations unies sur le statut des réfugiés et des apatrides, signée à Genève le 28 juillet 1951, Recueil des traités des Nations unies, volume 189, page 137.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales (1950), signée à Rome le 4 novembre 1950.

Protocole relatif au statut des réfugiés (1967), signé à New York le 31 janvier 1967, Recueil des traités des Nations unies n° 8791, Vol. 606, p. 267.

Decreto legislativo del 19 novembre 2007, n. 251, Attuazione della direttiva 2004/83/CE recante norme minime sull'attribuzione, a cittadini di Paesi terzi o apolidi, della qualifica del rifugiato o di persona altrimenti bisognosa di protezione internazionale, nonché norme minime sul contenuto della protezione riconosciuta.

Directive 2011/95/UE du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale.

Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale.

Directive 2013/33/UE du Parlement européen et du Conseil du 26 juin 2013 établissant des normes pour l'accueil des demandeurs de protection internationale.

Loi 12/2009, du 30 octobre, réglementant le droit d'asile et la protection subsidiaire.

Règlement (UE) n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride.

Règlement (UE) 2024/1348 du Parlement européen et du Conseil du 14 mai 2024 établissant une procédure commune en matière de protection internationale dans l'Union et abrogeant la directive 2013/32/UE.

Cour européenne des droits de l'homme (1997), affaire H.L.R. c. France, arrêt (Grande Chambre) du 29 avril 1997.

Cour européenne des droits de l'homme (2012), *Hirsi Jamaa et autres c. Italie* Arrêt (Grande Chambre) du 23 février 2012.

Cour européenne des droits de l'homme (2015), affaire N. D. et N. T. c. Espagne, décision (troisième section) du 7 juillet 2015.

Cour européenne des droits de l'homme (2017), affaire N. D. et N. T. c. Espagne, arrêt (troisième section) du 3 octobre 2017.

Cour européenne des droits de l'homme (2020), affaire N.D. et N.T. c. Espagne, arrêt (grande chambre) du 13 février 2020.

Cour permanente de justice internationale (1933), Statut juridique du Groenland oriental, arrêt du 5 avril, série A./B., fascicule n° 53, Leyde : A. W. Sijthoff's Publishing Company.

Cour internationale de justice (2002), Affaire relative à la souveraineté sur Pulau Ligitan et Pulau Sipadan, arrêt du 17 décembre, numéro de vente 858.

Cour internationale de justice (2012), Questions relatives à l'obligation de poursuivre ou d'extrader (Belgique c. Sénégal), arrêt du 20 juillet 2012,

Cour permanente d'arbitrage de La Haye (1998), Souveraineté territoriale et étendue du différend (Érythrée et Yémen), sentence du 9 octobre, in *Recueil des sentences arbitrales internationales*, volume XXII pp. 209-332.

Tribunal pénal international pour l'ex-Yougoslavie (2001), Procureur c. Dragoljub Kunarac Radomir Kovac et Zoran Vukovic, jugement du 22 février 2001.

Audiencia Nacional (2018), arrêt 1441/2018, 15 mars 2018.



Article de recherche

LA GUERRE DE NIXON CONTRE LA DROGUE ET L'ESSOR DE LA SURVEILLANCE VIRTUELLE DES FRONTIÈRES AUX ÉTATS-UNIS

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

J. Luigi M. Kunz Saponaro
Chercheur doctorant à l'Université Carlos III de Madrid.
Master en géopolitique et études stratégiques.
Master en sécurité, défense et géostratégie.
jkunz@hum.uc3m.es

Reçu le 31/03/2025
Accepté le 21/05/2025
Publié le 27/06/2025

Citation recommandée : Kunz Saponaro, J. L. M. (2025). Nixon's war on drugs and the rise of virtual border surveillance in the United States. *Logos Civil Guard Magazine*, 3(2), p.p. 147-170.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

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

LA GUERRE DE NIXON CONTRE LA DROGUE ET LA MONTÉE EN PUISSANCE DE LA SURVEILLANCE VIRTUELLE DES FRONTIÈRES AUX ÉTATS-UNIS

Résumé: INTRODUCTION. 2. REVUE BIBLIOGRAPHIQUE SUR LES FRONTIÈRES ET LA SURVEILLANCE VIRTUELLE. 3. 3. LA THÉORIE DE LA SÉCURISATION EN TANT QUE CADRE THÉORIQUE 3.1. titre de la sous-section trois point un 3.2. 4. OPÉRATIONNALISATION ET MÉTHODOLOGIE 5. ANALYSE 5.1 . La création d'une question de sécurité par Nixon. 5.1.1 La création d'une guerre nationale contre la drogue. 5.1.2. la virtualisation de la frontière pendant le mandat de Nixon. 5.2. Résultats et effets appliqués de la sécurisation de Nixon 6. CONCLUSION. 7. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Cet article étudie l'évolution de la frontière entre les États-Unis et le Mexique, qui est passée d'une frontière historiquement symbolique à l'une des frontières les plus fortifiées et technologiquement avancées au monde. Les dernières décennies ont vu une transformation significative des pratiques de contrôle des frontières, caractérisée par l'intégration de mécanismes de surveillance numérique qui renforcent les barrières physiques traditionnelles. Cette étude aborde ce phénomène en explorant le lien entre la guerre contre la drogue de Nixon et la numérisation de la frontière entre les États-Unis et le Mexique pendant l'administration Nixon (1969-1974). Considérant la crise de la drogue comme une menace existentielle, la rhétorique du président Nixon a défini la drogue comme l'"ennemi numéro un", lançant ainsi sa guerre contre la drogue. C'est ainsi qu'a commencé un processus de sécurisation qui a permis d'allouer des ressources extraordinaires pour contrer cette menace nouvellement perçue. En utilisant la théorie de la sécurisation développée par l'école de Copenhague, le rôle joué par Nixon dans le cadrage de la menace sécuritaire est analysé afin d'élucider comment son discours a justifié la création de pratiques de contrôle des frontières virtuelles aux États-Unis. Les résultats suggèrent que la sécurisation de la crise de la drogue a fourni la base nécessaire à l'adoption de technologies de surveillance numérique innovantes. Cette recherche contribue au débat académique sur la numérisation des frontières et fournit un cadre méthodologique pour des études comparatives sur l'évolution virtuelle des frontières nationales.

Resumen: Este trabajo investiga la evolución de la frontera entre Estados Unidos y México, que pasó de ser históricamente un límite simbólico para convertirse en una de las fronteras más fortificadas y tecnológicamente avanzadas del mundo. En las últimas décadas se ha observado una transformación significativa en las prácticas de control fronterizo, caracterizada por la integración de mecanismos de vigilancia digital que refuerzan las barreras físicas tradicionales. El estudio que se presenta aborda este fenómeno explorando el nexo entre la Guerra contra las Drogas de Nixon y la digitalización de la frontera entre Estados Unidos y México durante la Administración Nixon (1969–1974). Al conceptualizar la crisis de las drogas como una amenaza existencial, la retórica del presidente Nixon definió las drogas como el “enemigo número uno”, iniciando así su Guerra contra las Drogas. Comenzó así un proceso de securitización que permitió asignar recursos extraordinarios para contrarrestar esta nueva amenaza percibida. Mediante el uso de la teoría de la securitización desarrollada por la Escuela de Copenhague, se analiza el papel desempeñado por Nixon al enmarcar la amenaza de

seguridad, con el fin de dilucidar cómo su discurso justificó la creación de prácticas de control fronterizo virtual en Estados Unidos. Los hallazgos sugieren que la securitización de la crisis de las drogas proporcionó la base necesaria para adoptar tecnologías innovadoras de vigilancia digital. Esta investigación contribuye al debate académico sobre la digitalización de fronteras y ofrece un marco metodológico para estudios comparativos sobre la evolución virtual de las fronteras nacionales.

Mots clés : Frontière entre les États-Unis et le Mexique, surveillance numérique, théorie de la sécurisation, guerre contre la drogue, administration Nixon.

Palabras clave: Frontera EE. UU.–México, Vigilancia Digital, Teoría de la Securitización, Guerra contra las Drogas, Administración Nixon.

1. INTRODUCTION

La frontière qui sépare les États-Unis du Mexique est l'une des plus longues au monde. Une série de montagnes, de déserts et de rivières caractérisent les 3 141 kilomètres de terrain qui séparent les deux pays. Les premières délimitations physiques de la frontière ont été introduites à la fin de la guerre américano-mexicaine de 1847, qui a débouché sur le traité de Guadalupe (voir Trist *et al.*, 2022). Les changements politiques introduits par ce traité ont été transférés sur le territoire par 52 monticules de pierre placés d'un océan à l'autre tout au long de la marge (US Customs and Border Protection, 2019). Beaucoup de choses ont changé depuis la séparation symbolique qui délimite la frontière sud des États-Unis (US). Aujourd'hui, elle est devenue l'une des frontières les plus fortifiées et technologiquement avancées qui soient.

L'aspect virtuel de cette frontière présente un intérêt particulier pour les pratiques de surveillance que les pays du monde entier mettent en œuvre pour sécuriser leurs frontières. En effet, le potentiel des systèmes de surveillance contemporains en termes de contrôle des frontières nationales a fait l'objet de nombreuses études jusqu'à récemment (voir Adams, 2001 ; Amore, Marmura, & Salter, 2008 ; Heyman, 2008). Cependant, on sait peu de choses sur le moment et la raison pour lesquels, en particulier, les États-Unis ont décidé d'entremêler les aspects physiques et virtuels de leurs frontières afin d'en améliorer le contrôle. Il s'agit là d'une parenthèse déconcertante, surtout si l'on considère la position dominante des États-Unis en termes d'arsenal numérique utilisé le long de la frontière américano-mexicaine, et que l'on ne sait guère où tout cela a commencé.

La recherche montre un lien entre la guerre du Viêt Nam et la mise en œuvre par les États-Unis de mécanismes virtuels d'application de la loi le long de la frontière entre les États-Unis et le Mexique (voir Barkan, 1972 ; Grandin, 2019 ; Rosenau, 2001). Toutefois, le lien entre ces deux événements distincts de l'histoire américaine n'a pas fait l'objet d'une attention suffisante. Pour être plus précis, le lien en question est la guerre contre la drogue de Nixon. C'est en décrivant la drogue comme l'ennemi numéro un des États et en déclarant une guerre totale contre la drogue en 1971 que le président a réussi à ouvrir une fenêtre pour la numérisation de la frontière méridionale. En répondant à la question de recherche suivante, cet article vise à combler cette lacune dans la littérature académique : comment la guerre contre la drogue sous l'administration Nixon a-t-elle contribué à la transition d'un contrôle physique de la frontière sud à des mécanismes virtuels d'application de la loi ?

La théorie de la sécurisation constitue un outil précieux pour répondre à cette question. Cette théorie a été développée par l'École de Copenhague et fournit un cadre théorique qui peut être utilisé pour identifier des modèles dans le processus de sécurisation d'une question qui fournit des ressources compensatoires extraordinaires. Dans cette recherche, ces modèles élucidés par l'un des principaux éléments de l'École, Wæver (1995), sont appliqués aux commentaires de Nixon sur la guerre contre la drogue et à l'investissement ultérieur dans des actifs numériques pour la frontière sud des États-Unis.

Cette étude soutient que le fait que Nixon ait présenté le discours sur la drogue comme une menace nationale a permis aux États-Unis d'avancer dans la virtualisation de la frontière américano-mexicaine. La période analysée dans cet article coïncide avec le mandat de l'administration Nixon, c'est-à-dire 1969-1974. Établir à quel moment précis

et de quelle manière les États-Unis ont réussi à lancer leur fortification virtuelle de la frontière est précieux pour le débat académique. En effet, les résultats de cette recherche peuvent être utilisés pour comparer les développements technologiques dans les études frontalières d'autres pays, également pendant leurs phases initiales de virtualisation des frontières.

Afin de développer la recherche avec diligence, ce document est divisé en plusieurs sections. La première section présente l'analyse documentaire des approches théoriques les plus pertinentes qui ont été adoptées pour mener des études sur les frontières virtuelles. La deuxième section présente la théorie de la sécurisation comme le cadre théorique adopté par cette étude pour mener à bien son analyse. La troisième section résume l'opérationnalisation et la méthodologie utilisées pour formaliser cette recherche. La quatrième section est consacrée à l'analyse de cette étude. Dans cette section, les principes de la théorie de la titrisation sont appliqués à deux des discours emblématiques de Nixon. Les conclusions qui en découlent sont ensuite discutées en s'appuyant sur des sources secondaires. La dernière section propose une conclusion qui résume les résultats et les considérations obtenus tout au long de cette étude.

2. ANALYSE DE LA LITTÉRATURE SUR LES FRONTIÈRES ET LA SURVEILLANCE VIRTUELLE

Un certain nombre de théories sont utilisées pour apprécier les différents fondements des frontières et leurs modèles de transformation. En ce qui concerne spécifiquement les processus de virtualisation des frontières, le champ des théories applicables est considérablement plus restreint. Pour identifier ce qui a été écrit sur la relation entre les frontières et leur numérisation en fonction des besoins politiques, quatre théories principales parviennent à attirer l'attention. Cette section est consacrée à la discussion de ces différentes contributions académiques. Chacune d'entre elles apporte un éclairage différent sur le sujet de recherche de l'étude et peut être utilisée pour en comprendre l'origine.

Michel Foucault a encouragé l'adoption d'une perspective plus philosophique dans les études de surveillance. En examinant la théorie du philosophe français, Lemke (2015) a affirmé que " le travail de Foucault sur la gouvernementalité offre non seulement des perspectives importantes pour une analyse de l'État, mais fournit également des outils analytiques pour étudier la relation entre le libéral et les technologies de sécurité " (p. 5). Plus précisément, la théorie foucaldienne de la gouvernementalité décrit la manière dont les États emploient le pouvoir par le biais de techniques disciplinaires et de surveillance plutôt que par la force directe (Lemke, 2015). Cette théorie analyse la dimension extraterritoriale du contrôle des frontières géré par les acteurs étatiques, qui peut aller au-delà de la démarcation physique de leur propre pays.

Cette idée est intéressante pour comprendre la numérisation des frontières, car elle peut être appliquée aux pratiques des États qui luttent contre les menaces pour la sécurité nationale en réinterprétant les démarcations physiques. L'idée sous-jacente à cette théorie est d'essayer de bloquer des risques spécifiques avant qu'ils n'atteignent la frontière. Pour être plus précis, les lois nationales peuvent être utilisées pour pousser à des changements gouvernementaux qui prévoient l'informatisation des questions de sécurité qui menacent la sécurité nationale. De cette manière, les États peuvent évoluer vers un système de surveillance de plus en plus virtuel, utilisé pour contrôler et éliminer les dangers avant

qu'ils ne parviennent à pénétrer sur leur territoire (voir Armstrong, 1992 ; Paden, 1984). Cette série d'actions met en évidence la façon dont les frontières conventionnelles peuvent changer une fois que les configurations virtuelles sont intégrées dans les pratiques de contrôle des frontières.

La théorie foucaldienne de la gouvernementalité est toutefois insuffisante lorsqu'elle est appliquée à l'étude de la sécurisation des frontières liées à la drogue. Bien que la théorie mentionne l'agence technologique dans la création des frontières, elle est principalement orientée vers une étude de la surveillance et du contrôle plutôt que vers la sécurisation des frontières *en tant que telle*. Cette théorie n'est pas en mesure d'expliquer pourquoi les décideurs politiques agissent lorsqu'ils sont confrontés à des événements imprévus, comme ce fut le cas lors de la crise de la drogue des années 1960 aux États-Unis. Dans le même ordre d'idées, Kerr (1999) conclut que la théorie ne peut "rendre compte de l'évolution des limites du gouvernement, si ce n'est en soulignant le simple fait que le gouvernement échoue souvent en raison de résultats imprévus" (p. 196). Ainsi, bien que cette gouvernementalité foucaldienne se soit révélée pionnière dans la virtualisation des frontières, elle ne permet pas d'apporter une réponse exhaustive à la question de recherche qui guide la présente étude.

Le déterminisme technologique est une autre théorie pertinente utilisée pour analyser les frontières intelligentes. Cette théorie repose sur l'identification des développements technologiques en tant que moteurs sociaux et politiques. Elle souligne en particulier l'importance de la technologie dans l'élaboration des changements politiques. Selon Smith (1994), "le pouvoir de la technologie [est] un agent de changement crucial [qui] occupe une place prépondérante dans la culture de la modernité" (p. ix). Selon cette théorie, ce ne sont pas les personnes qui sont à l'origine des nouveautés, mais la technologie elle-même. Celle-ci entraîne à son tour des changements qui sont d'abord inscrits à l'ordre du jour politique, puis mis en œuvre par les décideurs.

De cette manière, les transformations des frontières sont considérées comme le résultat d'avancées technologiques plutôt que d'impulsions sociopolitiques. En ce sens, l'essor de la surveillance électronique, du suivi biométrique et de la télédétection a d'abord rendu viable la répression virtuelle. Ainsi, en reliant cette perspective à la question de recherche de cet article, les stratégies de répression des drogues ont évolué en fonction des possibilités technologiques plutôt que des décisions politiques. Par conséquent, les décideurs politiques américains ont été poussés, plutôt que d'être à l'origine d'un changement technologique, à mettre en œuvre la répression virtuelle aux frontières pour lutter contre l'entrée de drogues dans le pays.

Bien que le déterminisme technologique parvienne à fournir des informations pertinentes sur l'évolution des régimes frontaliers, il a été critiqué pour avoir trop simplifié ce processus. Il est largement avancé que les membres sociaux et politiques sont également capables d'influencer la technologie plutôt que d'être à sa merci. En d'autres termes, une meilleure compréhension de la technologie a permis de la contrôler (Dafoe, 2015, p. 1049 ; Lynch, 2008). Par conséquent, l'aspect numérique des frontières n'est pas le résultat d'une dynamique technologique, mais est contrôlé par les politiciens. Ainsi, l'adaptation de la frontière sud des États-Unis pendant le mandat de Nixon peut être considérée comme un virage technologique clair. Toutefois, ce tournant a été contrôlé par des actions menées par des hommes, ce qui fait qu'il est difficile de s'appuyer sur un déterminisme technologique pour la recherche proposée dans cet article.

La composition numérique des frontières peut également être comprise à travers la théorie des frontières de Nail. Cette théorie propose une vision de la frontière qui considère que les frontières physiques conventionnelles sont de plus en plus mobiles et dispersées. Selon Nail (2016), "la frontière n'est pas réductible à la définition classique des limites d'un État souverain" (p. 2). Selon l'auteur, les frontières évoluent inévitablement vers une identité informationnelle ou numérique qui affecte la compréhension sociale d'un pays. Cela signifie que les frontières ont pris une forme virtuelle, car les problèmes modernes affectent la circulation transfrontalière des personnes et des biens, ce qui nécessite des réponses actualisées. Dans le cas du trafic de drogue aux États-Unis, par exemple, les nouvelles méthodes adoptées par les cartels ont nécessité des actions innovantes de la part du contrôle des frontières américaines pour contrer cette tendance. Dans les années 1960 et 1970, ces actions se réduisaient à la transformation des frontières en espaces de contrôle en réseau.

La théorie des frontières contourne donc la conception conventionnelle des frontières en tant que telles. Plutôt que de se concentrer exclusivement sur leur aspect territorial et physique, comme l'élucide Sharma (2023, pp. 163-164), il est nécessaire d'étendre cette conception aux actifs intangibles qui composent les frontières des États. Les implications de cette théorie ajoutent une nouvelle dimension au pouvoir des gouvernements. En effet, les frontières ne doivent pas être considérées comme une simple ligne, mais comme une vaste zone entourant la démarcation physique (Nails, 2016). En effet, les États peuvent aller bien au-delà de leurs frontières physiques grâce à des mécanismes d'application virtuels dans le but de sécuriser leurs frontières. Les bases de données de la patrouille frontalière américaine et les réseaux d'échange de renseignements, qui ont été largement utilisés pour sécuriser la frontière méridionale, en sont des exemples concrets. Dans les années 1970, ces systèmes de patrouille frontalière ont conduit à des expansions qui ont ouvert la voie aux structures numériques actuelles de contrôle des frontières.

La théorie des frontières défend l'idée que les États peuvent surveiller les mouvements au-delà de leurs propres frontières. Selon cette conception, les délimitations territoriales perdent de leur pertinence lorsque les gouvernements prennent des mesures liées à la surveillance des frontières (Sharma, 2023, p. 164). Bien qu'ils représentent toujours un aspect important de l'élaboration des politiques frontalières, les gouvernements ont tendance à agir au-delà de la délimitation territoriale afin d'intercepter les menaces potentielles. En d'autres termes, la prévention devient aussi importante que la dissuasion physique. Les pièges de cet état d'esprit sont les interventions politiques extraterritoriales qui sont susceptibles de nuire aux relations internationales. Cette théorie est utile pour comprendre l'évolution générale de la conceptualisation de la frontière sud des États-Unis. Toutefois, elle peut être utilisée pour étudier la séparation sociale, bien qu'elle n'ait pas de lien clair avec les questions de sécurité frontalière.

Pour comprendre les frontières d'un point de vue sécuritaire, il faut prendre en compte la théorie de la sécurisation de l'école de Copenhague. Otukoya (2024, p. 1750) a observé que la création d'un problème de sécurité peut être la clé de la création de ressources extraordinaires utilisées pour protéger une nation d'un danger imaginaire. Cette théorie est utile pour comprendre comment les caractéristiques numériques sont utilisées pour renforcer l'aspect physique de la frontière. L'accent est mis ici, entre autres, sur les capteurs de mouvement, la vidéosurveillance et tout autre élément technologique utilisé pour renforcer la police des frontières territoriales. Il est donc présenté comme le

cadre théorique approprié nécessaire pour identifier de tels modèles le long de la frontière méridionale des États-Unis.

Si l'on se réfère aux débuts de la guerre contre la drogue, des manœuvres telles que l'opération Intercept, lancée en 1969, ont été justifiées comme une action nécessaire pour lutter contre l'ennemi public numéro un de l'Amérique à l'époque. Dans le cadre de cette opération, de nouvelles formes de surveillance électronique des frontières sont devenues nécessaires pour la première fois dans l'histoire du régime frontalier américain. Ces besoins incarnent les piliers fondamentaux de la dimension technologique complexe qui caractérise la frontière américaine contemporaine. Étant donné le lien étroit entre cette théorie de la sécurisation et les objectifs de cette recherche, il est nécessaire d'en préciser la composition. Dans la section suivante, la théorie de la titrisation est résumée. Elle fournit des indicateurs clés pour comprendre comment la sécurisation de la frontière américaine a évolué sous l'administration Nixon en adoptant un aspect virtuel.

3. LA THÉORIE DE LA TITRISATION COMME CADRE THÉORIQUE

La théorie de la sécurisation est un cadre utile qui peut être utilisé pour comprendre la sécurité des frontières aux États-Unis pendant la présidence Nixon. La fonction générale de cette théorie est d'expliquer comment les enjeux en viennent à orienter le processus décisionnel d'un pays dans des domaines tels que le contrôle des frontières. Appliquée à l'étude en question, cette théorie semble être d'une grande aide pour comprendre les mécanismes de contrôle virtuels que les États-Unis ont ajoutés à leur frontière physique méridionale. En appliquant la théorie de la sécurisation à ce sujet, cette étude cherche à élucider le rôle joué par le président Nixon dans la mise en œuvre d'une frontière virtuelle. Cette section est consacrée à la présentation des principaux principes de la théorie de la sécurisation afin de les appliquer formellement à l'analyse du document.

L'école de Copenhague a fondé sa théorie sur cinq piliers principaux. Les piliers en question sont (1) la sécurisation en tant qu'acte de langage, (2) le cadrage élitiste des menaces, (3) l'exigence d'acceptation par le public, (4) l'identification de l'objet référent, et (5) la réversibilité et la désécurisation. Tous ces facteurs combinés peuvent être utilisés dans l'analyse de ce document pour découvrir comment la guerre américaine contre la drogue a contribué à la transition du contrôle physique des frontières vers des mécanismes virtuels d'application de la loi. Toutefois, avant d'entrer dans l'analyse, chaque indicateur est résumé et mis en contexte afin de clarifier la manière dont il est utilisé dans le cadre de l'étude de cas.

Déclarer qu'un problème constitue une menace pour la sécurité est un acte performatif entrepris par un gouvernement. Avec cette conception de la sécurité, Ole Wæver - le maître d'œuvre de la théorie de la sécurisation - découvre un acte performatif que les gouvernements entreprennent lorsqu'ils signalent au public la présence d'un problème lié à la sécurité (Wæver, 1995, p. 52). En attirant l'attention sur un problème, une élite peut accomplir un acte qui ouvre une fenêtre pour des mesures politiques exceptionnelles afin d'arrêter un revers particulier. Il importe peu que cette question représente un problème ordinaire ou une menace réelle pour la sécurité nationale. Ce qui compte, c'est que le public accorde aux représentants de l'État une liberté d'action considérable qui légitime leurs actions. C'est ce qu'on appelle un acte de langage.

Les actes de langage reposent sur la création verticale de la confiance entre les représentants de l'État et les citoyens. Le succès d'un acte de langage dépend de la mesure dans laquelle une promesse ou une déclaration est acceptée par le public. Les représentants de l'État profitent du sentiment de confiance que les citoyens leur accordent pour créer une nouvelle réalité politique dont l'existence dépend de la question de la sécurité conçue. C'est par l'utilisation d'actes de langage que la légitimation de prendre des mesures pour faire face aux menaces à la sécurité est révélée. Cette légitimation permet à son tour de mobiliser le déblocage des ressources de l'État en créant des actions qui vont au-delà des procédures normales et permettent la formation de mesures extraordinaires (Wæver, 1995, p. 53).

Cependant, cette pratique n'est pas sans risque. Wæver (1995) souligne qu'il en est ainsi parce qu'elle rend difficile la distinction entre l'acte et le degré réel de menace auquel un pays est confronté (p. 6). En d'autres termes, l'État peut devenir victime de son propre récit en accordant trop d'importance à une question qui, en réalité, ne présente pas de danger réel pour la sécurité de la nation. Ce faisant, il peut avoir l'effet inverse, à savoir compromettre la sécurité du pays en se concentrant trop sur un problème inexistant et en négligeant ses véritables priorités.

Le deuxième indicateur retrouvé dans la théorie de la sécurisation est la pratique des élites consistant à encadrer les menaces. La théorie de la sécurisation souligne l'influence que les acteurs clés exercent sur les actions politiques. Ce processus est initié par les quelques élus qui ont une influence significative dans les rangs politiques supérieurs. Une fois que ces personnes ont réussi à créer un récit de la menace, elles ont le pouvoir de définir ce qui peut être considéré comme des dangers existentiels pour la sécurité du pays. Il en résulte une action cohérente de l'État visant à s'attaquer au problème découlant de la création de ce même récit.

Cependant, l'autorité exercée par l'élite est une arme à double tranchant. D'une part, elle permet à l'État de réagir rapidement (Wæver, 1995, p. 54). Ceci est particulièrement positif, car les États sont souvent limités par une bureaucratie alambiquée qui prolonge considérablement le temps de mise en œuvre des mesures officielles. D'autre part, cette domination permet aux élites de contourner les processus démocratiques conventionnels (Wæver, 1995, p. 54). Cela signifie qu'en accélérant le processus normalement lent d'élaboration des politiques, seuls quelques privilégiés concentrent le pouvoir de décision entre leurs mains. Cette concentration du pouvoir permet à l'élite de décider non seulement de la manière de traiter les menaces à la sécurité, mais aussi de décider ce qui doit être considéré comme une menace et ce qui ne doit pas l'être. Ainsi, la formulation des questions de sécurité peut facilement être liée aux intérêts stratégiques des élites (Wæver, 1995, p. 54). En d'autres termes, les élites peuvent décider si elles agissent pour garantir la sécurité publique ou leurs intérêts personnels.

Cela nous amène au troisième indicateur : l'exigence d'acceptation par le public. Selon l'école de Copenhague, les mesures de sécurisation dépendent de leur acceptation par les publics concernés. Les principaux publics d'intérêt pour l'élite sont l'opinion publique, les organes législatifs ou les partenaires internationaux. Tous - qu'ils soient ou non indépendants - doivent s'appuyer sur la véracité du récit de la menace construit pour créer l'*élan* nécessaire à la mise en œuvre d'actions concrètes. Celles-ci, selon Wæver (1995, p. 53), permettent à leur tour de trouver une solution à la menace proposée. Sans l'acceptation du public, même les affirmations les plus convaincantes en matière de

sécurité risquent de s'effondrer. Par conséquent, la non-acceptation d'une question de sécurité est contre-productive et génère un processus de désacralisation. Les efforts de l'élite s'évanouissent alors au détriment de ses intérêts stratégiques (Wæver, 1995, pp. 53-54). C'est pourquoi l'indicateur de la demande d'acceptation du public est proposé comme un facteur essentiel. Il est nécessaire d'analyser dans quelle mesure l'approbation ou la défiance du public à l'égard de procédures inhabituelles peut autoriser ou contrarier l'éloignement des pratiques démocratiques traditionnelles.

Le quatrième indicateur qui compose la théorie de la sécurisation peut être identifié avec l'identification de l'objet de référence. Le processus de titrisation nécessite une spécification claire de ce qui est en jeu. Ce qui est en jeu dans ce cas est appelé l'objet de référence. Selon Wæver (1995, p. 52), l'objet de référence est généralement identifié à l'intégrité de l'État, à la souveraineté ou à la sécurité de ses citoyens. Le processus de définition de l'objet de référence est crucial pour la mobilisation des ressources. En effet, une délimitation claire de l'objet dessiné par les acteurs de la sécurisation débloque les moyens matériels nécessaires pour défendre cette entité particulière contre une prétendue coercition existentielle (Wæver, 1995, pp. 52-53). Cette définition claire est fondamentale pour justifier le recours à des actions exceptionnelles, car elle détermine ce qui doit être défendu par tous les moyens.

La réversibilité et la désécurisation constituent l'indicateur ultime de la théorie de la titrisation. Selon l'école de Copenhague, la sécurisation est sujette à des changements constants. Lorsque le public se rend compte qu'une menace pour la sécurité n'est plus existentielle, il peut annuler les mesures de sécurisation prises jusqu'à présent et replacer la question dans un débat politique normal (Wæver, 1995, p. 55). Cette rétractation permet à l'élite qui a encadré la question d'être mise en échec. Cette réversibilité met en évidence la façon dont les réponses d'urgence temporaires peuvent être démantelées après avoir connu une montée en puissance momentanée. C'est pourquoi Wæver (1995, pp. 54-55) a suggéré que l'acte de titrisation comporte des risques intrinsèques qui sont inhérents au processus de titrisation. En d'autres termes, les actions de titrisation peuvent facilement aller et venir, ce qui rend difficile la prévision des futures actions de sécurité qu'un gouvernement pourrait prendre.

En général, les principes qui constituent la théorie de la titrisation proposée par l'école de Copenhague sont des outils d'analyse précieux. C'est particulièrement le cas pour le sujet de recherche de ce document. L'application des outils analytiques mis à disposition par cette théorie peut faciliter la compréhension de la façon dont la guerre contre la drogue a pu être transformée en une question de sécurité utilisée pour créer un espace pour des mesures exceptionnelles. En effet, les principes énumérés dans cette section permettent d'évaluer la transformation des pratiques criminelles conventionnelles - telles que la contrebande et la consommation de drogues - et des problèmes de santé en mesures exceptionnelles adoptées par les États pour faire face à ces problèmes. Des changements politiques significatifs ont été apportés par les discours des élites qui ont abouti à des politiques sans précédent conduisant à l'adoption de mécanismes virtuels d'application de la loi pour lutter contre le trafic de stupéfiants le long de la frontière sud des États-Unis. La section suivante présente l'opérationnalisation et la méthodologie que ce document adopte pour mener à bien son analyse.

4. OPÉRATIONNALISATION ET MÉTHODOLOGIE

Toshkov (2016, p. 100) a décrit l'opérationnalisation comme la traduction de concepts abstraits en notions concrètes qui peuvent être observées, classées et mesurées empiriquement. Les principes qui composent la théorie de la sécurisation peuvent être utilisés dans le même but. Ce document a opérationnalisé quatre des cinq concepts clés pour comprendre le rôle de la guerre contre la drogue dans la transition des États-Unis vers des frontières virtuelles. Les quatre indicateurs qui composent la théorie et qui sont utilisés dans ce document pour analyser l'étude de cas sont : (1) la sécurisation en tant qu'acte de langage, (2) le cadrage élitiste des menaces, (3) l'exigence d'acceptation par le public et (4) l'identification de l'objet référent. Le dernier principe énoncé dans la théorie de la sécurisation - la réversibilité et la désacralisation - n'est pas utile pour cette recherche. En effet, ce dernier principe est utile pour étudier la déconstruction d'une mesure de sécurité, un aspect que cette étude n'a pas l'intention de couvrir. Toutefois, cela ne compromet pas la robustesse de ce travail, car les schémas menant à la titrisation restent inchangés.

Les quatre indicateurs nous permettent d'approfondir la dimension virtuelle que la frontière sud des États-Unis a acquise pendant le mandat de Nixon. Par conséquent, une réflexion qualitative critique sur le sujet de la recherche est encouragée afin de comprendre l'importance actuelle pour les États-Unis de renforcer la numérisation le long de leur frontière territoriale avec le Mexique. Les cinq indicateurs sont donc d'une importance fondamentale pour déterminer pourquoi la crise de la drogue a réussi à incarner un facteur clé dans les mécanismes d'application des frontières virtuelles.

La méthodologie de ce travail doit également être clarifiée. Cette recherche consiste en une étude de cas unique. Plus précisément, elle analyse la frontière sud des États-Unis pendant la présidence de Nixon. Les études de cas uniques permettent de fournir des informations précises sur un cas spécifique afin de créer des connaissances qui peuvent ensuite être appliquées à des cas similaires. En d'autres termes, avec cette recherche, le modèle de recherche peut ensuite être utilisé dans des cas similaires pour identifier des modèles analogues d'évolution dans le contrôle virtuel des frontières. La décision d'opter pour cette étude de cas repose sur le fait que les États-Unis sont l'un des premiers pays à avoir décidé d'opter pour la numérisation partielle de leurs frontières. Par conséquent, le choix de l'étude de cas se justifie par l'intérêt d'ajouter de nouvelles informations aux lacunes de la recherche universitaire sur ce sujet.

Une variété de sources primaires et secondaires est utilisée tout au long de l'analyse du sujet. L'objectif de disposer d'un large éventail d'informations provenant de sources variées permet de consolider et d'assurer la qualité des conclusions de cette recherche. Comme pour les sources primaires, les déclarations politiques, les articles de journaux et les discours publics sont pris en compte. Des éléments importants de la théorie de la titrisation peuvent être reconnus dans ces sources. Les sources secondaires utilisées dans cette étude proviennent d'études universitaires réalisées sur le thème de la sécurité des frontières, de la sécurité virtuelle et de la guerre contre la drogue. Il s'agit d'une pratique utile qui permet de situer les résultats de l'étude dans un débat académique plus large.

L'analyse du discours constitue l'épine dorsale de cette étude. Elle examine les informations tirées de deux discours prononcés par Nixon en relation avec la guerre contre la drogue. Basée sur une méthode qualitative, l'interprétation des sources données permet

d'identifier les indicateurs présentés dans le cadre théorique. Les discours politiques prononcés par le président américain sont donc essentiels pour mener à bien cette étude. De plus, en appliquant cette méthode de recherche, il est possible de tester la théorie utilisée dans cette étude. En effet, en appliquant les indicateurs proposés par la théorie de la titrisation aux discours, il est possible de comprendre s'il existe effectivement des modèles dans les discours politiques qui peuvent conduire à la titrisation des risques construits.

Le cadre temporel de cette recherche est basé sur le mandat de l'administration Nixon. Plus précisément, la période considérée s'étend de 1969 à 1974. Ce cadre temporel étroit permet de prendre en compte un certain nombre de mesures clés prises par le président américain de l'époque en ce qui concerne les mécanismes de contrôle virtuel le long de la frontière entre les États-Unis et le Mexique.

5. ANALYSE

5.1. LA CRÉATION D'UN PROBLÈME DE SÉCURITÉ PAR NIXON

La surveillance de la frontière américano-mexicaine entre 1969 et 1974 était principalement axée sur le commerce illégal de la drogue. La région de Sinaloa, dans le nord-ouest du Mexique, a commencé à cultiver de l'opium à partir d'immigrants chinois dans les années 1910. Depuis lors, le cartel de Sinaloa s'est enrichi en exportant cette substance principalement vers les États-Unis. Toutefois, avec la génération hippie et le trafic de marijuana, l'importation illégale de substances aux États-Unis est devenue un problème pour la société (Grillo, 2013, p. 255). Le problème de la drogue est devenu la question centrale autour de laquelle le président Nixon a basé la majeure partie de son activité politique. En outre, Timmons (2017, p. 15) a attiré l'attention sur le fait que Richard Nixon est devenu le premier président à promettre de fermer la frontière américano-mexicaine aux drogues illégales. En effet, alors que la guerre au Viêt Nam se poursuit, " l'administration Nixon américanise discrètement la technologie de la guerre, et la guerre sur le front intérieur s'intensifie " (Barkan 1972, p. 1).

Afin d'approfondir le rôle de Nixon dans le lancement de cette tendance, la première partie de l'analyse est consacrée à l'analyse de deux des discours du président en question. Il s'agit de *Remarks About an Intensified Program for Drug Abuse Prevention and Control* et de *Special Message to the Congress on Drug Abuse Prevention and Control*. Les deux discours ont été prononcés le 17 juin 1971. Les deux discours ont eu lieu le même jour et se sont succédé. En fait, le premier incarne la conférence de presse tenue pour expliquer ce qu'il a mentionné lors de son discours au Congrès.

Ces deux discours sont essentiels pour comprendre comment le cadre élitiste d'une menace a été proposé aux audiences politiques et publiques. En les examinant de près, il est possible de comprendre comment Nixon est parvenu à débloquent des ressources extraordinaires pour contrer la nouvelle menace existentielle de la drogue aux États-Unis. Les deux discours sont présentés ensemble dans un document fourni par le ministère américain de la défense (2017). Après avoir identifié les points les plus pertinents des deux discours, nous allons clarifier l'importance de ces mesures uniques dans le processus de virtualisation de la frontière sud des États-Unis entre 1969 et 1974.

5.1.1 Créer une guerre nationale contre la drogue

Lorsque l'on examine les discours de Nixon du point de vue de la théorie de la sécurisation, il est nécessaire de rechercher un acte performatif. Cet acte doit attirer l'attention de l'auditoire sur l'existence d'un problème de sécurité qui met en péril son bien-être. C'est ce qu'a fait le président Nixon en déclarant avec audace une guerre totale contre la drogue. Lors de sa conférence de presse, après avoir adressé un message spécial au Congrès, il a commencé sa communication en déclarant que "l'ennemi public numéro un aux États-Unis est la toxicomanie" (US Department of Defense, 2017, p. 1). Cette ouverture grandiloquente était captivante pour le public. Elle a contribué à créer un sentiment de peur au sein de la population américaine, 15 ans après la catastrophique guerre du Viêt Nam. Il n'est pas surprenant que toute référence aux menaces pour la sécurité nationale, aux guerres et aux ennemis dans ces années-là ait facilement suscité des sentiments de paranoïa et un désir d'agir.

Pour proposer cette nouvelle menace, Nixon a dû indiquer en quoi elle consistait réellement. Il l'a fait en déclarant que :

Il existe plusieurs grandes catégories de drogues : celles de la famille du cannabis, comme la marijuana et le haschisch ; celles utilisées comme sédatifs, comme les barbituriques et certains tranquillisants ; celles qui élèvent l'humeur et suppriment l'appétit, comme les amphétamines ; et les drogues comme le LSD et la mescaline, qui sont souvent appelées hallucinogènes. Enfin, il y a les analgésiques narcotiques, comme l'opium et ses dérivés, la morphine et la codéine. L'héroïne est fabriquée à partir de la morphine". (Département de la défense des États-Unis, 2017, p. 10).

C'est ce que la théorie de la sécurisation identifie avec l'identification de l'objet référent. En désignant et en insistant sur qui ou quoi représente une menace, le public peut identifier le problème et faire pression pour que des mesures soient prises à son encontre.

En outre, le fait de se présenter comme un président prudent a contribué à rendre l'acte performatif plus convaincant. Ainsi, il déclare : " J'hésite toujours à apporter une nouvelle responsabilité à la Maison Blanche, [...] mais je pense que c'est un problème tellement urgent [...] qu'il fallait l'apporter " (US Department of Defense, 2017, p. 2). Ce faisant, Nixon cherche à se présenter comme le protecteur et le garant des États-Unis dont les actions sont guidées par les besoins des citoyens américains et non par des intérêts personnels.

Une série de mesures exceptionnelles ont été créées pour faire face à cette menace pour la sécurité nationale. Nixon affirme qu'"une nouvelle offensive totale doit être menée" (US Department of Defense, 2017, p. 1), évoquant la nécessité d'un effort commun pour stopper un danger qui a réussi à pénétrer sur le sol américain. Ces propos précisent à quel point les États-Unis sont déterminés à lutter activement contre les menaces sécuritaires liées à la drogue. La mise en œuvre de mesures de guerre, telles que le déploiement et la création de départements militaires et fédéraux chargés de contrôler et de combattre les routes de la drogue vers les États-Unis, constitue la base de ce nouveau plan d'action.

À ce stade, il est nécessaire de souligner l'acceptation par le public du discours de Nixon. En fait, on peut dire que le public a accepté le discours de Nixon sur la guerre

contre la drogue. Les signes de cette acceptation sont une série d'actions proposées par l'administration et mises en œuvre avec le soutien général de la majorité du pays. L'opération la plus emblématique qui a initié la guerre contre la drogue est l'opération Interdiction lancée en septembre et octobre 1969. Cette opération a abouti à la fermeture presque complète de la frontière entre les États-Unis et le Mexique.

L'opération Interdiction s'est soldée par une débâcle en raison de l'impossibilité de contrôler l'ensemble de la frontière par une disposition physique. Bien que deux mille agents des douanes aient été déployés, aucun résultat efficace n'a été obtenu (voir Reid, 2022). Néanmoins, le soutien public et politique a donné lieu à de nouvelles actions qui ont ouvert la voie à de nouveaux types de procédures. C'est le cas du Comprehensive Drug Abuse Prevention and Control Act (CDAPC Act) de 1970, adopté pour renforcer le contrôle des États-Unis, entre autres, le long de la frontière méridionale.

L'opération Interdiction et la loi CDAPC constituent les jalons sur lesquels reposent ses discours de 1971. En fait, ces actions ont déclenché une série de procédures gouvernementales supplémentaires visant à intensifier la guerre contre la drogue. Le passage suivant donne une idée de la manière dont le président Nixon souhaitait renforcer ces procédures visant à mettre un terme à cette menace pour la sécurité : "Nous devons maintenant reconnaître franchement que les procédures délibérées mises en œuvre dans le cadre des efforts actuels de lutte contre la toxicomanie ne sont pas suffisantes en elles-mêmes. Le problème a pris les dimensions d'une urgence nationale " (US Department of Defense, 2017, p. 3). C'est ainsi qu'il a pu obtenir un soutien bipartisan pour faire face à cette nouvelle menace sécuritaire apparemment dévastatrice.

Pour être plus précis, les mesures législatives les plus importantes adoptées depuis les deux discours analysés dans cette section sont les suivantes : la création par décret de l'Office of Special Action for the Prevention of Drug Abuse en 1971, l'extension du Drug Addict Rehabilitation Act de 1966 en 1971, l'organisation de l'International Security Assistance Act de 1971 avec l'International Development and Humanitarian Assistance Act de 1971, la création de l'Office of Drug Abuse Law Enforcement en 1972 et la création de la Drug Enforcement Administration (DEA) en 1973.

Il est important de souligner que de telles actions n'ont été possibles qu'avec un large soutien politique. Le président était conscient de cette caractéristique, puisque tout au long de sa conférence de presse, il a insisté à plusieurs reprises sur le soutien bipartisan dont bénéficiaient ses actions. Il s'agit là d'un aspect important dans le cadre de la théorie de la sécurisation, car il met en évidence le pouvoir que l'acceptation générale confère à l'élite qui définit la menace pour la sécurité. Ce pouvoir permet à l'élite de prendre des mesures extraordinaires à brève échéance, ce qui va à l'encontre des longues procédures bureaucratiques qui sont ignorées dans de telles situations.

Au-delà du soutien politique, Nixon a réussi à faire accepter à la société la menace qu'il avait réussi à mettre en place. Il l'a fait en soulignant à quel point chaque membre de la société américaine était affecté par la menace de la drogue. En déclarant qu'"en 1960, il y a eu moins de 200 décès dus aux stupéfiants dans la ville de New York. En 1970, ce chiffre était passé à plus de 1 000" (US Department of Defense, 2017, p. 2), Nixon a réussi à établir une relation verticale entre l'auteur de l'acte de langage et son public. L'argument avancé par le président américain est que la population américaine moyenne tombait dans la drogue. Il s'agit d'un argument convaincant auquel les gens peuvent s'identifier, car cela

se passe près d'eux. Les efforts déployés pour convaincre son public illustrent un autre aspect fondamental mentionné dans la théorie de la titrisation. Il montre comment les membres de l'élite tentent de créer un problème et de le faire reconnaître par un large public.

Une situation similaire est décrite dans le même discours, dans lequel Nixon tente d'appeler à une réponse communautaire en s'appuyant sur des sentiments individuels. La phrase en question est la suivante : "Pour vaincre cet ennemi, qui cause tant d'inquiétude, et à juste titre, à tant de familles américaines, de l'argent sera fourni" (US Department of Defense, 2017, p. 1). Ce que le président américain a cherché à faire ici, c'est s'assurer la faveur ultime de son auditoire. C'est par le biais de déclarations de ce type que la légitimation est obtenue et doit donc être considérée comme une partie inhérente du processus de cadrage de la menace dans la titrisation.

Le processus de légitimation était nécessaire pour prendre des mesures aux frontières des États-Unis et au-delà. Comme il l'a déclaré : "Aucune attaque sérieuse contre notre problème national de drogue ne peut ignorer les implications internationales d'un tel effort, et l'effort national ne peut réussir sans s'attaquer au problème sur un plan international", puis "Je lance une escalade mondiale de nos programmes existants de contrôle du trafic de stupéfiants" (US Department of Defense, 2017, p. 11). Ces actions visaient principalement ceux qui introduisaient clandestinement de la drogue sur le sol américain. Selon les termes du président, il s'agit "d'arrêter le trafic de drogue en frappant les producteurs de drogues illégales [...] et le trafic de ces drogues à travers nos frontières" (p. 4). En d'autres termes, Nixon a présenté les trafiquants de drogue étrangers comme une menace en élargissant le champ d'action de ceux qui étaient à l'origine de la menace qui mettait en péril la sécurité des États-Unis. Il s'agit là de questions clés qui façonneront désormais les relations extérieures du pays, en particulier avec les États situés en deçà de sa frontière méridionale.

Les discours utilisés pour cette analyse du discours ont permis d'identifier les modèles proposés par la théorie de la sécurisation. En s'adressant au Congrès et au public américain dans les discours suivants, le président Nixon a réussi à relancer la transformation du problème de la drogue en une question de sécurité persistante. Ainsi, les marqueurs de la théorie de la titrisation ont permis de retracer l'évolution d'un problème criminel et de santé publique relativement conventionnel vers un problème nécessitant des changements politiques substantiels. Afin de développer le processus de sécurisation entrepris par les États-Unis pour introduire des mécanismes virtuels d'application de la loi à leur frontière territoriale méridionale entre 1969 et 1974, la section suivante examine un certain nombre de sources secondaires qui ont été écrites sur ce sujet.

5.1.2 La virtualisation de la frontière sous l'administration Nixon

La première mesure concrète pour lutter contre la contrebande de drogue du Mexique vers les États-Unis a été prise par le président Richard Nixon en 1969 avec l'opération Intercept. Selon Grillo (2013), cette opération consistait à fouiller "chaque véhicule ou piéton traversant la frontière sud tandis que les militaires installaient des unités radar mobiles entre les postes" (p. 256). Ce plan s'est avéré être un fiasco, car il est rapidement apparu qu'un contrôle au sol aussi exhaustif était utopique. Le personnel sur le terrain n'était tout simplement pas en mesure de sceller l'ensemble de la frontière avec le Mexique. Comme l'a fait remarquer Ghaffaray (2019), la frontière séparant les États-Unis

du Mexique était trop large et son orographie trop injustifiée pour être clôturée dans son intégralité. Pour cette raison, l'opération Intercept, qui a coûté 30 millions de dollars, n'a duré que 17 jours.

Cependant, Mendoza (2023) note que Nixon a décidé de fortifier la frontière avec une clôture virtuelle, et non physique, afin d'obtenir de meilleurs résultats dans la réduction des flux de drogue. En d'autres termes, constatant que la fermeture physique de la frontière était à elle seule un projet chimérique, Nixon a investi dans la structure de contrôle frontalier existante afin d'améliorer la sécurisation de la frontière d'un point de vue technologique. En outre, Koslowski (2019) explique qu'à l'époque, le gouvernement américain a déployé des capteurs de mouvement, infrarouges, sismiques et magnétiques capables de détecter à la fois les mouvements et la chaleur à une distance de 50 à 250 pieds. La justification utilisée par Nixon pour légitimer l'investissement dans les mécanismes numériques allait dans le sens de la protection de la frontière commune avec le Mexique : la guerre contre la drogue.

Les besoins de Nixon coïncidaient avec les intérêts des entreprises militaires américaines de haute technologie. La fin imminente de la guerre du Viêt Nam a contraint ces entreprises à se diversifier et à commencer à investir dans des systèmes destinés à soutenir l'armée américaine. Pour ce faire, elles devaient convaincre le gouvernement américain de continuer à investir dans différents types de dépenses militaires, c'est-à-dire dans une défense menée au niveau national et non plus uniquement au niveau international. Ainsi, à partir de la fin des années 1960, plusieurs entreprises de recherche et développement engagées par les États-Unis pour soutenir l'intervention militaire au Viêt Nam ont réussi à signer des contrats fédéraux.

Sylvania Electronics, par exemple, a réussi. Plus précisément, elle a vendu au gouvernement américain, en 1970, ses capteurs terrestres utilisés pour détecter à distance les mouvements sur le terrain. Il s'agit d'un événement pionnier, car il symbolise la première application des technologies virtuelles utilisées pour surveiller la frontière sud des États-Unis. Grandin (2019) précise que ces capteurs ont été industrialisés dans le cadre du plan du secrétaire à la défense Robert McNamara visant à construire une clôture virtuelle et physique séparant le Nord et le Sud du Viêt Nam et qu'ils ont été utilisés pour détecter les mouvements de troupes et de camions le long de la piste Ho Chi Minh. La principale fonction de ces capteurs était de détecter les activités sismiques provoquées par le passage de personnes ou de camions à proximité des capteurs et le déplacement du sol (Rosenau, 2001, pp. 11-12). Cette technologie était également utile pour détecter les mouvements à travers et à proximité de la frontière américaine, c'est pourquoi elle a été mise en œuvre pendant le mandat de Nixon.

Un autre élément technologique utilisé pour la première fois pendant la guerre du Vietnam et plus tard à la frontière américano-mexicaine était les drones. Selon Novak (2015), ces drones étaient connus sous le nom de RPV (Remotely Piloted Vehicles) - alors qu'aujourd'hui ils sont connus sous le nom de Unmanned Aerial Vehicles (UAV) - et étaient utilisés pour scanner la zone depuis le ciel. Décrivant la frontière mexicaine de 1972, Novak explique que :

Les drones *QU-22b* et les drones de l'armée de l'air américaine - qui étaient excédentaires au Viêt Nam en raison de l'introduction de drones plus sophistiqués - ont

été renvoyés aux États-Unis, où ils [ont survolé] la frontière pour surveiller les capteurs et relayer les données aux points de contrôle centraux (Novak, 2015).

Avec l'avènement des drones, un centre de surveillance a été créé pour recevoir les informations recueillies par les UAV. Barkan (1972, p. 1) explique que ces drones survolent des parties éloignées de la frontière pour relayer les signaux de centaines de capteurs au sol qui sont ensuite envoyés au Centre de surveillance des infiltrations, où de gros ordinateurs diagnostiquent les données.

5.2 Résultats et effets appliqués de la titrisation Nixon

La guerre du Viêt Nam représente une étape importante dans la sécurisation virtuelle de la frontière entre les États-Unis et le Mexique sous la présidence de Nixon. En effet, l'application des technologies de guerre aux frontières intérieures des États-Unis a clairement évolué, entraînant une virtualisation de la frontière. Ces développements se sont avérés utiles à l'administration Nixon pour alimenter le désir de mener la guerre contre la drogue. Cela s'est accompagné d'un engagement politique croissant en faveur de l'étanchéité de la frontière (), un terme normalement utilisé dans les missions militaires, mais pour la première fois lié à la frontière américaine à l'époque (Lee, 2005), l'un des principaux objectifs étant d'empêcher les trafiquants de drogue d'entrer par la frontière sud des États-Unis.

Bien que les systèmes de surveillance mis en place par l'administration Nixon n'aient pas toujours fonctionné - comme l'a souligné sans relâche Barkan (1972, p. 2), "ils sont incapables de distinguer l'ami de l'ennemi" -, ils ont indéniablement constitué une étape importante dans le contrôle de la frontière américaine. Cette innovation s'est avérée être la pierre angulaire de presque tous les présidents suivants en ce qui concerne la gestion de la frontière sud des États-Unis. Le fait qu'une nouvelle tendance aussi importante soit basée sur un acte performatif, tel que décrit par la théorie de la sécurisation, explique l'importance de la création de menaces pour la sécurité dans la perception du public dans la promotion des mesures de sécurité.

Comme cela a été débattu des décennies après la guerre contre la drogue, il n'y avait en fait pas de menace liée à la drogue, ou du moins pas dans la mesure où le président Nixon l'avait d'abord fait remarquer. John Ehrlichman, alors assistant du président pour les affaires intérieures sous Nixon, a admis que l'administration mentait à propos de la menace de la drogue pour permettre des actions politiques et militaires (voir López, 2016). Quoi qu'il en soit, il existait un réel problème de drogue au sein des armées américaines à l'étranger et loin du sol américain (voir Vulliamy, 2011).

L'adoption d'une approche sécuritaire de la frontière entre les États-Unis et le Mexique, initiée par Nixon, a des conséquences connexes. Il est nécessaire d'examiner la littérature sur l'utilisation des allégories comme moyen de polarisation. Celles-ci élucident en effet la relation entre la sécurisation, les actes de langage et la création de luttes sociales dans le cadre du processus plus large de justification de la surveillance des frontières et des pouvoirs d'urgence. C'est le cas de Kruglanski (2007), qui s'est concentré sur l'idée de métaphores pour illustrer comment le langage est capable de cadrer les menaces en déterminant le processus de réponse politique. Le discours de l'"ennemi numéro un" de Nixon coïncide avec la métaphore guerrière de Kruglanski. Plus précisément, les métaphores de guerre de Nixon reflètent celles du discours de Kruglanski

(2007) sur le terrorisme. Cela suggère que la sécurisation de la frontière américaine a été utilisée même à une époque plus récente. Dans les deux cas, la réponse totalisante a été rendue possible par la légitimation de mesures d'urgence telles que la surveillance des frontières.

Les inconvénients d'une telle approche dans le processus de sécurisation des États-Unis résident dans ses effets de polarisation et de radicalisation à long terme. Par exemple, Moyano *et al.* (2016) ont critiqué le processus de sécurisation de l'ère Bush (la guerre contre la terreur) provoqué par l'acte terroriste du 11 septembre. Selon eux, la société américaine aurait davantage bénéficié d'un récit moins polarisant qui aurait évité les disjonctions sociales qui affectent la fracture sociale actuelle. On peut dire la même chose de l'approche de Nixon concernant la guerre contre la drogue. En effet, en suivant cette idée, en présentant la question comme une guerre plutôt que comme un défi humain, il a éclipsé les problèmes de santé publique et de développement communautaire qui se posaient aux États-Unis. Il aurait donc été souhaitable d'adapter la conception de ses actes discursifs. À long terme, il aurait été plus rentable d'opter pour une réponse plus holistique. Celles-ci auraient dû être basées sur une approche multidisciplinaire afin d'éviter les contrecoups créés par des processus de sécurisation qui ne prennent en compte qu'une seule question.

6. DÉBAT

Ce document visait à répondre aux questions de recherche suivantes : comment la guerre contre la drogue menée par l'administration Nixon a-t-elle contribué à la transition du contrôle physique de la frontière sud vers des mécanismes virtuels d'application de la loi ? Pour répondre à cette question, cette recherche s'est appuyée sur les grands principes qui constituent la théorie de la sécurisation. Ces principes ont été utilisés comme indicateurs pour effectuer une analyse du discours de deux discours prononcés par Nixon dans lesquels il a officiellement déclaré sa guerre contre la drogue. Il ressort de cette analyse que le président Nixon a activement participé à la formulation d'une menace sécuritaire proposée à son auditoire public et politique comme portant atteinte à la sécurité nationale du pays tout entier. Grâce à l'acceptation par le public du récit donné, des mesures extraordinaires ont été prises pour stopper l'entrée des drogues dans les États. Parmi ces mesures, il a été possible d'identifier l'introduction de mécanismes virtuels d'application de la loi.

Des recherches antérieures ont souligné l'importance de la frontière virtuelle dans la définition de la frontière sud des États-Unis. Heyman (2008) a souligné comment les murs et les clôtures sont renforcés par l'aspect virtuel qui définit l'aspect coercitif de la politique d'immigration américaine. Une idée avancée par Amoores *et al.* (2008, pp. 99-100) lorsqu'ils énumèrent l'ensemble des technologies utilisées pour aider la patrouille frontalière américaine à classer, au moyen d'algorithmes, ce qui peut être considéré comme une menace et ce qui ne peut pas l'être. Son étude s'est donc concentrée sur l'évolution du rôle de l'homme dans la gestion des frontières, ainsi que sur la capacité des États-Unis à exercer un contrôle au-delà de la frontière physique grâce à l'aspect virtuel de celle-ci. Un autre type de recherche sur la virtualisation de la frontière américaine est lié au développement militaire. Comme le suggère Adams (2001), les progrès militaires dans l'utilisation de la technologie pour mener la guerre ont été utilisés pour revigorer la frontière intelligente séparant les États-Unis du Mexique afin d'assurer une surveillance optimale.

Au vu de ces recherches, une lacune est apparue dans la littérature. En effet, si la sécurisation, la virtualisation et la militarisation de la frontière sud des États-Unis ont été étudiées, le début de cette transformation n'a pas été suffisamment pris en compte. L'objectif de ce document était précisément de combler cette lacune. Après avoir mené cette recherche, il est apparu clairement que la présidence de Nixon s'est avérée révolutionnaire pour l'histoire de la gestion des frontières aux États-Unis. En effet, c'est la première fois que les États ont mis en œuvre des éléments technologiques - tels que des capteurs terrestres et les premières versions de drones - pour surveiller la frontière entre les États-Unis et le Mexique. En comblant cette lacune dans le débat académique sur les origines de la frontière intelligente pour les États, il est possible de faire progresser la recherche et la comparaison sur les frontières du point de vue des études de sécurité. De plus, en testant la théorie de la sécurisation pour mener à bien une analyse du discours tenu par les élites politiques pour définir les besoins en matière de sécurité, les résultats de cette recherche peuvent également être appliqués à d'autres cas. Par exemple, il serait possible d'appliquer cette recherche à des cas similaires tels que la frontière espagnole partagée avec le Maroc. La théorie de la sécurisation utilisée dans cette étude pourrait permettre de comprendre comment et quand les mécanismes de frontières virtuelles ont été introduits dans le régime frontalier espagnol.

Cependant, il est également nécessaire de mentionner les limites de ce travail. Si le choix d'une étude de cas unique était nécessaire pour fournir une description précise du rôle de Nixon dans la virtualisation de la frontière entre les États-Unis et le Mexique, une étude comparative aurait pu permettre une compréhension globale des frontières en général. De même, l'utilisation d'une méthode mixte pour mener à bien cette étude pourrait également accroître la validité des résultats. L'intégration d'une perspective quantitative dans l'approche qualitative privilégiée dans cette recherche pourrait fournir des informations importantes pour localiser les parties des frontières qui ont été les plus fortifiées par rapport au processus de virtualisation.

Les limites de ce travail représentent toutefois une opportunité de stimuler la recherche sur ce sujet. Comparer les résultats de cette étude avec d'autres cas où des progrès significatifs ont été réalisés dans la virtualisation des frontières dans le cadre d'un processus de fortification plus général. Les villes autonomes espagnoles de Ceuta et Melilla, par exemple, pourraient bénéficier de ce type d'analyse. La compréhension de leur processus de fortification des frontières depuis leur adhésion à l'espace Schengen fournirait des informations importantes sur la manière dont la gestion des frontières a changé en raison des pratiques de frontières virtuelles. Déterminer si le début de cette numérisation a été complété par l'exemple fourni précédemment par les États-Unis pourrait aider à concevoir les frontières de Ceuta et Melilla d'une manière plus complète. En outre, l'application de la théorie de la sécurisation à ces cas spécifiques pourrait révéler la double importance du récit national qui justifie ce changement de régime frontalier, parallèlement au récit mis en œuvre par l'Union européenne. Il serait ainsi possible d'analyser l'idée de la Forteresse Europe du point de vue de la sécurisation virtuelle.

Dans l'ensemble, les tentatives de Nixon pour lutter contre la contrebande de drogue à la frontière sud des États-Unis ont jeté les bases de décennies de politique frontalrière entre les États-Unis et le Mexique. L'importance de ce changement dans le régime frontalier est visible dans le *modus operandi* actuel de la patrouille frontalrière. Il serait pratiquement impossible de maintenir le contrôle de la frontière sud sans les technologies militaires américaines utilisées au Viêt Nam et introduites à la frontière nationale sous

Nixon. En retraçant les origines du contrôle virtuel des frontières jusqu'à la guerre contre la drogue de Nixon, cette étude révèle comment la politique de sécurité peut tranquillement transformer l'architecture même des frontières d'un pays.

RÉFÉRENCES BIBLIOGRAPHIQUES

- Adams, J. (2001). Virtual defence. *Foreign Affairs*, 80(3), 98-112.
- Amoore, L., Marmura, S. et Salter, M. B. (2008). Frontières intelligentes et mobilités : Zoned spaces, enclosures. *Surveillance & Society*, 5(2).
- Armstrong, W. G. (1992). Punition, surveillance et discipline dans le Paradis perdu. *Lost. Studies in English Literature, 1500-1900*, 32(1), 91-109. <https://doi.org/10.2307/450942>
- Barkan, R. (1972, 18 février). Ils vous observent, à travers les murs, dans l'obscurité de la nuit alors que vous marchez, et cela vient du Viêt Nam. *Free Press*.
- Dafoe, A. (2015). Sur le déterminisme technologique : une typologie, des conditions de portée et un mécanisme. *Science, Technology and Human Values*, 40(6), 1047-1076. <http://www.jstor.org/stable/43671266>
- Ghaffary, S. (2019, 16 mai). Le mur "plus intelligent" : comment les drones, les capteurs et l'intelligence artificielle patrouillent la frontière. *patrouillent la frontière. Vox*.
- Grandin, G. (2019, 9 février). Comment les États-Unis ont assemblé le mur frontalier. *The Intercept*.
- Grillo, I. (2013). Les cartels mexicains : un siècle au défi de la politique antidrogue des États-Unis. *The Brown Journal of World Affairs*, 20(1), 253-265. <http://www.jstor.org/stable/24590897>
- Heyman, J. McC. (2008). Constructing a Virtual Wall : Race and Citizenship in U.S.-Mexico Border Policing". *Journal of the Southwest*, 50(3), 305-333.
- Kerr, D. (1999). Decapitating the King and Enthroning the Market : A Critique of Foucauldian Governmentality. *Science & Society*, 63(2), 173-202.
- Koslowski, R. K. (2019, 29 mai). *Réformes de l'immigration et sécurité des frontières. frontières. Articles.* <https://items.ssrc.org/border-battles/immigration-reforms-et-technologies-de-la-sécurité-des-frontières/>
- Kruglanski, A. W., Crenshaw, M., Post, J. M. et Victoroff, J. (2007). What Should This Fight Be Called ? Metaphors of Counterterrorism and Their Implications. *Psychological Science in the Public Interest*, 8(3), 97-133. <http://www.jstor.org/stable/40062365>
- Lee, J. (2005, 31 août). James H. Scheuer, 13-term New York congressman, is dead at 85. *The New York Times*.
- Lemke, T. (2015). *Foucault, governmentality and critique*. Routledge.
- López, G. (2016, 22 mars). *Nixon official : The real reason for the war on drugs was to criminalize blacks and hippies (La vraie raison de la guerre contre la drogue était*

de criminaliser les noirs et les hippies). Vox.
<https://www.vox.com/2016/3/22/11278760/war-on-drogues-racisme-nixon>

Lynch, M. (2008). *Ideas and perspectives*. Dans *The Handbook of Science and Technology Studies*, édité par Hackett, E. J., Amsterdamska *Technology Studies* édité par Hackett, E. J., Amsterdamska, O., et Wajcman, J., 9-11. Cambridge, MA : MIT Press

Mendoza, M. E. (2023, 30 octobre). *L'histoire du mur frontalier entre les États-Unis et le Mexique*. Le temps. <https://time.com/6324599/bidens-trump-history-border-wall/>

Moyano, M., Bermúdez, M. I. et Ramírez, A. (2016). La psychologie positive face à la radicalisation et au terrorisme ? Une analyse du discours d'Obama au Caire. *Escritos De Psicología - Psychological Writings*, 9(3), 53-58.
<https://doi.org/10.24310/espsiescpsi.v9i3.13219>

Nail, T. (2016). *Frontier theory*. Oxford University Press.

Novak, M. (2015, 24 septembre). Comment la guerre du Viêt Nam a amené la surveillance high-tech aux États-Unis. Gizmodo.

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research*, 11(1), 1747-1755. <https://doi.org/10.30574/ijrsra.2024.11.1.0225>

Paden, R. (1984). Surveillance et torture : Foucault et Orwell sur les méthodes de discipline. *Social Theory and Practice*, 10(3), 261-271.

Reid, Justin M. "An Exercise in International Extortion' : Operation 'Intercept' and Nixon's 1969 War on Drugs". Mémoire de maîtrise, Chapman University, 2022.
<https://doi.org/10.36837/chapman.000412>

Sharma, V. (2023). Examen de la "théorie de la frontière" de Thomas Nail. New Zealand Journal of Asian Studies.

Smith, M. R., & Marx, L. (Eds.) (1994). *Does technology drive history ? Le dilemme du déterminisme technologique*. Mit Press.

Timmons, P. (2017). Trump's Wall on Nixon's Border : How Operation Intercept laid the groundwork for decades of U.S.-Mexico border policy, including Donald Trump's wall. *NACLA Report on the Americas*, 49(1), 15-24.
<https://doi.org/10.1080/10714839.2017.1298238>.
<https://doi.org/10.1080/10714839.2017.1298238>

Toshkov, D. (2016). *Research design in political science*. Basingstoke : Palgrave Macmillan.

Trist, N., Cuevas, L., Couto, B. et Atristain, M. (2022). The Treaty of Guadalupe Hidalgo. Dans G. M. Joseph & T. J. Henderson (Eds.), *The Mexico Reader : History, Culture,*

Politics (pp. 599-603). Duke University Press.
<https://doi.org/10.2307/j.ctv2rr3g8m.96>

Douanes et protection des frontières des États-Unis (2019). *Saviez-vous que... Des obélisques centenaires marquent la frontière entre les États-Unis et le Mexique...* U.S. Customs and Border Protection. <https://www.cbp.gov/about/history/did-you-know/obelisk>

Département de la défense des États-Unis (2017). *41 Nixon Remarks Intensified Program for Drug Abuse*. Gouvernement des États-Unis.

Vulliamy, E. (2011, 23 juillet). *La "guerre contre la drogue" de Nixon a commencé il y a 40 ans, et la bataille fait rage*. The Guardian.
<https://www.theguardian.com/society/2011/jul/24/war-on-drugs-40-years>

Wæver, O. (1995). Securitization and Desecuritization. Dans R. D. Lipschutz (Ed.), *On Security* (pp. 46-87). Columbia University Press.



Article de recherche

VIOLENCES SEXUELLES COMMISES PAR DES INCONNUS À MADRID ET BARCELONE: UNE ANALYSE SITUATIONNELLE

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

Francisco Pérez Fernández

Docteur en philosophie et en sciences de l'éducation, professeur associé (psychologie criminelle, psychologie de la personnalité et histoire de la psychologie), départements de psychologie et de criminologie et sécurité, faculté des sciences de la santé des hôpitaux HM, université Camilo José Cela.

fperez@ucjc.edu

ID. ORCID : 0000-0002-3039-2397

Google Scholar : https://scholar.google.es/citations?hl=es&user=O_7qrwgAAAAJ

Heriberto Janosch

Docteur en sciences juridiques et économiques,
Professeur d'histoire de la psychologie et des bases biologiques du comportement, Faculté de santé,
Université UNIE

heriberto.janosch@universidadunie.com

ID. ORCID : 0000-0002-0188-2434

Google Scholar : <https://scholar.google.com/citations?user=uA4iKy0AAAAJ>

Enrique López López

Magistrat de l'Audience nationale d'Espagne.
Professeur de droit constitutionnel et de droit de la procédure pénale, Faculté des sciences juridiques et des relations internationales, Université UNIE

enrique.lopezl@universidadunie.com

Francisco López-Muñoz

Docteur en médecine et en chirurgie et docteur en langue et littérature espagnoles, professeur de pharmacologie et vice-recteur pour la recherche et les sciences, faculté des hôpitaux HM des sciences de la santé, université Camilo José Cela.

flopez@ucjc.edu

ID. ORCID : 0000-0002-5188-6038

Google Scholar : <https://scholar.google.es/citations?user=IbuwtWgAAAAJ&hl=es>

Reçu le 28/03/2025

Accepté le 23/05/2025

Publié le 27/06 /2025

Citation recommandée : Pérez, F, Janosch, H, López, E et López, F (2025). Violence sexuelle par des inconnus à Madrid et Barcelone : une analyse situationnelle. *Revista Logos Guardia Civil*, 3(2), p.p. 171-196.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

VIOLENCES SEXUELLES COMMISES PAR DES INCONNUS À MADRID ET BARCELONE: UNE ANALYSE SITUATIONNELLE

Résumé: INTRODUCTION. 2. HYPOTHÈSE. 3. MÉTHODOLOGIE. 4. RÉSULTATS. 5. DISCUSSION. 6. CONCLUSIONS. 7.

Résumé : Les agressions sexuelles, en tant que crimes particulièrement victimisants et médiatisés, suscitent l'inquiétude, la préoccupation et l'intérêt du public. Par conséquent, elles sont souvent à l'épicentre du débat général sur la politique pénale. Par conséquent, les agressions sexuelles et leurs protagonistes - délinquant et victime - ne sont pas toujours analysés de manière adéquate, traités et compris en dehors des environnements criminologiques, policiers et juridiques. De même, la recherche criminologique elle-même, ainsi que les développements législatifs, juridiques et pénitentiaires liés au sujet - nécessairement controversés - ont souvent tendance à se fondre dans des généralités théoriques difficiles à confronter et même à concilier avec des faits et des cas particuliers qui, lorsqu'ils sont étudiés en détail, semblent impossibles à intégrer dans les cadres explicatifs généraux disponibles. La présente étude, basée sur l'approche de la Théorie de l'Action Situationnelle (TAS) proposée par Wikström et ses collaborateurs et sur l'analyse qualitative et quantitative des sentences judiciaires prononcées dans les provinces de Madrid et de Barcelone, vise à montrer comment les écosystèmes criminels dans lesquels les délits sont commis modifient substantiellement leur déroulement, ainsi que les actions de l'agresseur et de sa victime. Un fait qui peut s'avérer extrêmement utile comme outil d'enquête policière et d'analyse comportementale, ainsi que pour la compréhension des événements criminogénétiques et des dynamiques criminelles spécifiques.

Resumen: Las agresiones sexuales, en tanto que delitos de especial significación victimal y mediática, suscitan gran alarma, preocupación e interés públicos. En consecuencia, suelen formar parte del epicentro del debate general en torno a las políticas criminales. Ello motiva que las agresiones sexuales y sus protagonistas -agresor y víctima- no siempre sean adecuadamente analizados, tratados y entendidos fuera de los entornos criminológicos, policiales y jurídicos. Del mismo modo, la propia investigación criminológica, así como el devenir legislativo, jurídico y penitenciario vinculados al tema -necesariamente controvertido-, tienden a menudo a difuminarse en generalidades teóricas que cuesta confrontar e incluso encajar con hechos y casos particulares que, al estudiarse en detalle, parece imposible de encajar en los marcos explicativos generales de que se dispone. El presente estudio, que se realiza partiendo del enfoque aportado por la Teoría de la Acción Situacional (TAS), propuesta por Wikström y sus colaboradores, y se vale del análisis cualitativo y cuantitativo de sentencias judiciales emitidas en las provincias de Madrid y Barcelona, pretende mostrar cómo los ecosistemas criminales en que se cometen los delitos, modifican sustancialmente su curso, así como las acciones del agresor y su víctima. Un hecho que puede ser extremadamente útil como herramienta para la investigación policial y el análisis de conducta, así como para la comprensión de eventos criminogénéticos y dinámicas criminales específicas.

Mots clés : agression sexuelle, théorie de l'action situationnelle, échelle multidimensionnelle, analyse du comportement.

Palabras clave: Agresión Sexual, Teoría de la Acción Situacional, Escalamiento Multidimensional, Análisis de Conducta.

1. INTRODUCTION

Les agressions sexuelles sont une source de souffrance pour les victimes . Cette situation est aggravée dans les cas qui, pour des raisons particulières, deviennent particulièrement "célestres" et suscitent l'intérêt de l'opinion publique. Le fait est que les agressions sexuelles, souvent très médiatisées, suscitent une grande inquiétude et un débat social, ce qui déclenche généralement des enquêtes et des procès particulièrement médiatiques qui ont un fort impact sur les victimes par le biais d'une victimisation secondaire et d'une *présence ex post*¹ (Gutiérrez de Piñeres, Coronel et Pérez, 2009 ; Domínguez Vela, 2016). Pour fournir quelques éléments de réflexion, il convient de rappeler que, selon l'annuaire statistique du ministère espagnol de l'Intérieur, en 2022, 19 013 délits contre la liberté sexuelle ont été "connus" par les forces et corps de sécurité de l'État (FCSE) - il s'agit de plaintes et d'enquêtes -, dont 11 426 étaient des abus/agressions sexuels et, parmi ceux-ci, 4 270 étaient des abus/agressions sexuels avec pénétration.² . L'une des modalités les plus fréquentes de ce type de délit est celle où l'agresseur sexuel, généralement un homme agissant seul, attaque une femme dans le hall d'entrée d'un immeuble résidentiel ou dans le garage, ce pour quoi il est communément appelé "portalero" (Janosch González, Pérez-Fernández et Soto Castro, 2020).

Quoi qu'il en soit, le "chiffre gris" des statistiques reflète les inquiétantes données policières, victimaires et judiciaires qui sous-tendent ce problème : l'élucidation des agressions sexuelles commises par des individus inconnus des victimes est plus complexe que dans les cas où il existe une forme de lien entre la victime et l'agresseur qui permet aux enquêteurs du FCSE d'identifier avec certitude l'agresseur et, le cas échéant, d'obtenir des preuves pouvant être utilisées comme éléments de preuve devant les tribunaux (Corovic, Christianson et Bergman, 2012 ; Janosch, Pérez-Fernández et Herrero, 2025). Il convient de garder à l'esprit que la dynamique cognitivo-comportementale de ces individus tend à fonctionner selon un processus d'escalade, ce qui implique que, par rapport à leur dangerosité potentielle, il est très possible qu'il existe un biais de sérialité - ou du moins de répétitivité - qui les amène à commettre plus d'une agression sexuelle au cours de leur carrière criminelle s'ils ne sont pas identifiés et arrêtés (Pueyo et Redondo Illescas, 2007). D'autant plus que, plutôt qu'un lien direct avec des troubles diagnostiqués plus ou moins graves, cette catégorie de délinquants semble être influencée par un amalgame complexe d'éléments socioculturels, de facteurs de stress de la vie et de structures de personnalité (Arqué-Valle et al., 2024).

D'autre part, et pour développer la dernière idée, il est bien connu que le contexte - environnement matériel et humain - dans lequel le délinquant agit modifie son comportement, de sorte que les stratégies et les ressources qui peuvent être parfaitement

¹ Ces deux types de victimisation sont souvent confondus. La victimisation secondaire concerne les coûts personnels et psychologiques que la victime doit supporter du fait d'être plus ou moins constamment exposée à des situations qui lui font revivre (ou se remémorer) le préjudice subi, et ce de manière répétée (Kühne, 1986). La victimisation *ex post* - également appelée victimisation de "quatrième niveau" - est déclenchée lorsque la personne éprouve du désespoir et de l'impuissance après n'avoir pas reçu l'aide attendue de la part des institutions et des professionnels en qui elle avait confiance (tels que la police, la santé, l'administration, la justice) et dont elle ne reçoit pas le soutien moral et matériel attendu (Triviño, Winberg et Moral, 2021).

² Au total, 14 555 crimes contre la liberté sexuelle ont été résolus, en comptant tous les types de crimes contre la liberté sexuelle, ce qui donne un total de 4 518 "chiffre gris" - crime ayant fait l'objet d'une enquête, mais non résolu - de 4 518 plaintes. En ce qui concerne les abus/agressions avec pénétration, le nombre de cas non résolus en 2022 était de 860 (ministère de l'intérieur, 2023).

utiles dans un certain endroit n'ont pas nécessairement la même valeur d'applicabilité dans un écosystème criminel-délinquant différent. Wikström, face à cette contingence, a développé ce que l'on appelle la théorie de l'action situationnelle de la causalité du crime (ou CAS), dont les propositions fondatrices ont été publiées entre 2004 et 2006 (Serrano Maíllo, 2017). Cette théorie tente d'intégrer, dans le cadre d'une théorie de l'action adéquate, les principaux résultats des formulations théoriques et de la recherche en criminologie, ainsi que les connaissances théoriques et empiriques des sciences sociales et comportementales en général. En effet, les corrélats de la criminalité sont assez bien connus, mais il n'y a guère d'accord sur les causes de la criminalité, qui se présentent comme un mélange confus d'éléments auxquels chaque chercheur attache plus ou moins d'importance en fonction de ses intérêts. Cela explique l'inflation de théories - et les contradictions internes - qui affectent les études criminologiques (Pérez-Fernández, Janosch et Popiuc, 2023).

En bref, la TAS affirme que les actes criminels peuvent être expliqués comme des processus - des mécanismes systémiques et interactifs, mais non déterministes - qui mobilisent des "actions" qui transgressent finalement des règles de conduite formelles ou informelles (Wikström, et al., 2012). Il s'agirait donc d'un sous-ensemble de comportements inclus dans l'ensemble plus général des *actes qui violent les règles de conduite morales*. Bien que ces constructions de conduite morale ne soient spécifiées dans aucune loi et ne constituent donc pas toutes des crimes en soi, elles pourraient répondre aux mêmes mécanismes que ceux qui mobilisent les crimes au sens juridique (Janosch González, 2013). En d'autres termes, la TAS définit le crime comme un acte qui enfreint une règle de conduite établie par la loi - insérée dans le code pénal de chaque État - et qui peut être analysé en termes d'*action morale*. L'action morale, à son tour, serait comprise comme une conduite guidée par des règles qui établissent ce qui, dans certaines circonstances - ou situations - spécifiques, serait bon ou mauvais à faire (Wikström et Treiber, 2016).

Définir le crime en ces termes, comme un acte qui viole une règle de conduite morale incarnée par des lois, présente l'avantage de pouvoir s'appliquer à n'importe quel type de crime, n'importe où et à n'importe quel moment. Ainsi, ce qui est défini est un acte de violation d'une règle de conduite morale qui est spécifiée sous la forme d'une loi particulière "donnée". On peut donc affirmer que la TAS est fondamentalement une théorie générale de l'action morale (Wikström, et al., 2012), car elle expliquerait toutes les actions morales, 2012), car elle expliquerait tous les types de violation des règles morales en tout temps et en tout lieu, en mettant l'accent sur le mécanisme induisant la violation des règles morales, plutôt que sur le contenu de la règle morale désobéie en tant que variable et sujette à une modification constante en fonction des variations de la loi positive particulière dans un espace-temps spécifique (Pauwels, 2018a ; Pauwels, 2018b). Le mécanisme causal de la perception et de l'action serait présent aussi bien dans les petits vols que dans les agressions sexuelles ou les homicides. Conséquence : les politiques pénales, à moyen et long terme, auraient plus de succès si elles visaient l'éducation en conformité avec la règle morale en vigueur, plutôt que la punition ou le simple contrôle (Pérez-Fernández, Janosch et Popiuc, 2023 ; Janosch, Pérez-Fernández, Popiuc et López-Muñoz, 2024).

En fin de compte, c'est l'interaction entre la propension au crime d'une personne donnée et les caractéristiques criminogènes du contexte qui déclenchera le processus qui aboutira - ou non - à l'acte criminel lui-même. La propension à commettre un délit dépend

des normes morales de la personne et de sa capacité à se maîtriser, sachant que cette capacité peut être altérée par la consommation d'alcool ou de drogues, ou par un stress intense accompagné d'un déséquilibre émotionnel. Ces caractéristiques criminogènes du scénario dépendront à leur tour de ce que l'on appelle l'"environnement moral" - celui perçu par l'individu plutôt que l'environnement réel - et de l'existence ou non de facteurs dissuasifs, qui encouragent ou découragent la violation des règles (Wikström, et al., 2012). Le corollaire de tout cela, en ce qui concerne cette étude, est clair : l'agresseur sexuel n'agira pas toujours de la même manière et en toute indépendance du lieu où il se trouve, car la situation générale dans laquelle il est inséré - qu'il faut analyser et comprendre - modifiera nécessairement sa perception des règles, ses considérations morales, son attention aux lois et aux restrictions et, finalement, son action délinquante (Pérez-Fernández, Popiuc et López-Muñoz, 2024).

Considéré de cette manière, on comprendra que pour le CAS, au-delà de toute idée discutable, la nationalité, l'idéologie politique, l'identification sexuelle ou la religion d'une personne ne sont pas en soi des causes de criminalité sous quelque forme que ce soit, ou du moins ne devraient pas être évaluées comme plus importantes que d'autres circonstances personnelles, telles que l'âge ou le niveau d'éducation, parce qu'elles ne sont en fait que des attributs de la personne qui, en outre, sont modifiables. De même qu'il n'est pas logique de dire qu'une personne est plus susceptible de commettre un crime parce qu'elle est plus grande, il n'est pas non plus logique de mettre l'accent sur d'autres attributs personnels qui, en outre, relèveraient du domaine controversé des droits et libertés individuels. Ainsi, des variables telles que la nationalité ou la religion devraient être évaluées avec la même rigueur que d'autres causes contribuant à différentes formes de criminalité reconnues dans la littérature, telles que la pauvreté, le niveau d'éducation, le fait de vivre dans des environnements criminogènes, le manque d'opportunités, la polyconsommation, l'absentéisme scolaire, une compagnie inappropriée, etc. (Pérez-Fernández, Janosch et Popiuc, 2023). En d'autres termes, tout comme il serait absurde de dire qu'une personne commet des crimes - ou n'en commet pas - en raison de la couleur de ses cheveux ou de son poids en kilogrammes, il est également incohérent d'affirmer qu'elle pourrait être amenée à commettre des crimes simplement parce qu'elle est née dans un certain pays, parce qu'elle partage un certain sentiment idéologique, parce qu'elle s'identifie à un genre spécifique ou parce qu'elle pratique une certaine religion (Janosch, Pérez-Fernández et Herrero Roldán, 2024).

1.1. UNE NOTE JURIDIQUE NÉCESSAIRE

Cette introduction se termine en rappelant un fait bien connu, à savoir qu'en Espagne, des changements relativement récents ont été apportés au Code pénal (CP) en ce qui concerne les crimes sexuels, qui sont venus modifier les différentes perspectives existantes en ce qui concerne l'approche policière et judiciaire du problème. Tout d'abord, et en lien avec le modèle TAS décrit plus haut, elles entraînent une modification des comptages statistiques - qui modifieront également les discours médiatiques futurs - dont les effets ne seront perceptibles qu'à moyen terme et, par conséquent, ouvrent de nouvelles perspectives sur la perception générale de la criminalité, ainsi que sur les politiques réactives d'action à son égard, dont les effets sont encore à venir. Il n'est donc pas inutile, pour anticiper la suite et contextualiser les résultats présentés ici, de donner un bref aperçu critique de ces changements.

La LO 10/2022, du 6 septembre, connue sous le nom de *Loi du seul oui est oui*, a entraîné un changement notable en ce qui concerne la prise en compte des délits contre la liberté sexuelle. Ce règlement a introduit des changements significatifs dans le CP, en particulier dans l'unification des délits d'abus et d'agression sexuels, la redéfinition du consentement et la modification des peines associées. Mais, outre ces nouveautés législatives, il a également suscité un débat intense en raison des réductions de peine qui ont eu lieu : 1205 réductions de peine, dont 121 libérations de prison (CGPJ, 2023). L'adoption de cette loi s'inscrit dans le contexte de la nécessité de renforcer la protection de la liberté sexuelle et de garantir une réponse globale à toutes les formes de violence sexuelle.

Avant l'entrée en vigueur de la LO 10/2022, le code pénal espagnol établissait une distinction entre les abus sexuels et les agressions sexuelles. L'abus se référait à des actes sans violence ni intimidation, tandis que l'agression impliquait l'utilisation de la violence ou de l'intimidation. Avec la nouvelle loi, cette distinction disparaît. Ainsi, tout acte sexuel sans consentement est considéré comme une agression sexuelle, qu'il y ait eu ou non violence ou intimidation. Cette unification vise à reconnaître que tout acte sexuel non consenti est une atteinte à la liberté sexuelle d'une personne.

La loi établit que le consentement n'est réputé exister que lorsqu'il a été librement exprimé par des actes qui, compte tenu des circonstances de l'espèce, expriment clairement la volonté de la personne. Cette définition place le consentement au centre des relations sexuelles, éliminant les interprétations qui pourraient justifier des comportements non consensuels. Cela implique que tout acte sexuel non consensuel est une agression, qu'il y ait ou non violence ou intimidation, car l'absence de consentement à elle seule implique une violence implicite. Bien que le consentement ne soit pas explicitement défini, cela ne signifie pas que la jurisprudence n'ait pas compris que ce consentement était substantiel, en tant qu'élément dans ce cas négatif du type, que l'agent a agi : 1) sans le consentement de la personne agressée sexuellement ; 2) par l'existence d'un consentement vicié par des circonstances concomitantes découlant de la position de l'auteur de l'acte, significativement dérivée de la parenté ou d'une situation équivalente, ou de la domination que sa position en tant que conséquence d'une relation de travail, de l'enseignement, de la supériorité, de l'ascendance, même en tant que conséquence d'une différence d'âge par rapport à la victime, pourrait restreindre l'autodétermination sexuelle de la victime ; et 3) que l'agent a profité d'une position de privilège découlant de la vulnérabilité ou de l'état d'inconscience de la victime³. Ces dernières séquences d'atteintes à la liberté sexuelle étaient auparavant classées dans la catégorie des abus sexuels, tandis que les cas où l'auteur agissait contre le consentement de la victime ouvraient la catégorie des agressions sexuelles, étant donné qu'elles étaient commises au moyen de la violence ou de l'intimidation, qui était la caractéristique requise pour une telle agression. Cependant, la concomitance de l'absence de consentement qui imprègne le titre qui englobe ces crimes a toujours été nécessaire, puisqu'il s'agit de crimes contre la liberté sexuelle, qui repose naturellement sur l'existence d'un consentement à la réalisation d'actions à contenu sexuel.

La formule utilisée aujourd'hui par le législateur est donc une formule ouverte, qui a déjà été prise en compte par la jurisprudence, dans des termes similaires, pour

3 Voir, par exemple : STS 3865/2024 ; SAP A 872/2018.

comprendre le consentement comme concomitant. La formule susmentionnée se fonde sur les actes, de sorte que "le consentement n'est réputé exister que lorsqu'il a été librement manifesté par des actes qui, compte tenu des circonstances de l'espèce, expriment clairement la volonté de la personne" (LO 10/2022). Par *actes*, il faut entendre toutes sortes de manifestations ou de signes de la personne qui va consentir, qu'ils soient verbaux, gestuels ou situationnels, mais ils doivent être considérés comme explicites. Ainsi, le consentement est construit comme positif et concluant, et doit être donné librement (implicitement, non vicié : il doit dépendre exclusivement de la volonté de la personne, comme dans tout crime dont l'objet générique de protection est la liberté dans n'importe laquelle de ses expressions).

La réforme motivée par l'approbation de la LO 10/2022 a également ajusté les peines associées aux délits sexuels. Par exemple, les agressions sexuelles sans pénétration étaient auparavant punies d'une peine de 1 à 5 ans de prison, alors que la nouvelle loi établit une fourchette de 1 à 4 ans. Dans le cas des agressions avec pénétration, la peine minimale est ramenée de 6 à 4 ans, tandis que la peine maximale reste de 12 ans. Ces modifications ont fait l'objet de controverses, notamment en raison de l'effet de leur application rétroactive au profit des condamnés. L'application rétroactive de la loi, principe de base du droit pénal lorsqu'une règle favorise le délinquant, a conduit à la révision de nombreuses condamnations définitives. Cet effet imprévu a suscité un débat intense sur la nécessité d'adapter la loi pour éviter des conséquences indésirables, ce qui a finalement été fait par la LO 4/2023, du 27 avril.

Il ne fait aucun doute que la loi organique 10/2022 a été guidée par un objectif louable de protection de la liberté sexuelle en unifiant les infractions et en mettant l'accent sur le consentement. Toutefois, la réduction des peines dans certains cas a mis en évidence la complexité de la réforme du CP, de sorte qu'il est essentiel que les changements futurs examinent en détail les implications pratiques des modifications législatives pour garantir une protection efficace des victimes et une punition adéquate des auteurs. La controverse décrite ci-dessus est née du fait que les limites maximales et minimales de la peine ont été abordées sans prévoir la possibilité d'introduire une disposition transitoire. Dans une démocratie, le CP est un instrument extrêmement important qui doit rester à l'écart des idéologies et du sectarisme.

2. HYPOTHÈSE

Il est vrai que la législation à appliquer est la même à Madrid et à Barcelone, et que les conditions de son application sont identiques, ce qui signifie que l'approche juridique initiale - et ses vicissitudes - sera fondamentalement la même. Cependant, si l'on prête attention au modèle TAS décrit ci-dessus, il devient clair que, en acceptant que le contexte dans lequel le délinquant potentiel développe ses activités modifie son comportement, cela implique que les stratégies et les ressources qui peuvent être parfaitement utiles dans la province de Madrid n'ont pas nécessairement la même valeur d'applicabilité dans un autre écosystème criminel-délinquant différent, comme celui de la province de Barcelone, dans lequel, en outre, il opère sous le contrôle de forces de police et de modèles pénitentiaires qui sont également différenciés.

Par conséquent, l'intérêt de cet article repose sur la formulation et l'étude d'une hypothèse de base : les agressions sexuelles perpétrées dans la province de Madrid doivent être, d'une certaine manière et dans la mesure où elles sont médiatisées par

différents modèles d'action situationnelle, significativement différentes des agressions sexuelles commises dans la province de Barcelone.

3) MÉTHODOLOGIE

Il est vrai que la recherche criminologique ne trouve pas de données suffisantes ou appropriées dans les différentes bases de données publiques en Espagne pour tester ses approches. Le problème, déjà largement critiqué par d'autres chercheurs, réside dans le fait que ces informations sont collectées à des fins publiques-administratives qui répondent aux compétences de l'organisme compétent, et donc prennent rarement en compte les besoins des chercheurs et tendent à répondre à d'autres critères qui ne sont pas cohérents avec les prétentions de la science (Linde et Aebi, 2021). Les informations fournies par le Centre de documentation judiciaire (CENDOJ) du Conseil général du pouvoir judiciaire (CGPJ) sont toutefois particulièrement exceptionnelles, car elles offrent des données non filtrées, ce qui permet aux chercheurs de les traiter en fonction de leurs besoins spécifiques. Cependant, compte tenu d'autres lacunes inhérentes à la nature même de cette base de données, la documentation qu'elle fournit doit être correctement catégorisée et filtrée, sur la base de critères de départ très spécifiques (Janosch, Pérez-Fernández, Nut et Marset, 2023). Enfin, les informations fournies par le CENDOJ sont anonymes, publiques et libres de droits.

Compte tenu de ce qui précède, 76 cas d'agressions sexuelles commises par un auteur initialement inconnu de la victime dans les provinces de Madrid et de Barcelone ont été analysés dans le cadre de cette étude, sur la base de l'analyse des décisions judiciaires publiées dans la base de données CENDOJ. La taille de l'échantillon correspond à une représentation du nombre total d'agressions sexuelles connues et jugées commises par des auteurs inconnus dans les provinces indiquées. Les critères d'inclusion définis sont les suivants :

1. L'agresseur sexuel était un homme inconnu de la victime jusqu'à au moins 24 heures avant le crime, et il agissait toujours seul.
2. La victime, toujours de sexe féminin, était âgée de 16 ans ou plus au moment de l'infraction.
3. Les cas sont légalement définis, dans la phrase elle-même, comme des "agressions sexuelles" (pénétration effective ou au moins tentative de pénétration avec un pénis, à travers le vagin, la bouche et/ou l'anus ; ou pénétration effective avec des doigts ou d'autres objets, à travers le vagin et/ou l'anus).

Sur la base de ces critères d'inclusion, 38 crimes ont été trouvés, par hasard, dans la province de Madrid et 38 dans la province de Barcelone. Les analyses ultérieures ont été effectuées à l'aide du logiciel statistique R version 4.4.2 (2024), *Pile of Leaves*, Copyright (C) 2024 The R Foundation for Statistical Computing. Bibliothèques utilisées : *vegan*, *ggplot2*, *ggrepel*, *cluster*, *factoextra*, *readxl*, *mclust* et *clue*.

3.1. CATÉGORISATION DES ARRÊTS

Afin de compiler correctement les données issues des jugements en vue d'une analyse statistique ultérieure, les critères et les nomenclatures décrits ci-dessous ont été respectés :

- Le casier judiciaire de l'accusé. Ceux-ci sont codés dans des variables appelées *Ag_Sex* (dossier judiciaire pour infraction sexuelle), *Ag_Theft* (dossier judiciaire pour vol), *Ag_Viol* (dossier judiciaire pour violence non sexuelle) et *Ag_Unesp* (dossier judiciaire pour infraction non spécifiée). Ces variables ont été codées dans la base de données de la manière suivante : 0 si le délinquant n'a pas d'antécédents ou de problèmes psychiatriques, 1 s'il en a, et 2 si aucun de ces éléments n'est mentionné dans la condamnation.
- Variables situationnelles spécifiques. Un groupe de sept variables répond à des circonstances situationnelles liées au viol lui-même - elles pourraient être considérées comme "scénographiques". La victime peut avoir résisté ou non à la commission du crime (*Ver_Resist*) ; elle peut avoir crié à l'aide ou non (*Ver_Shout*) ; des tiers, tels que d'éventuels témoins ou des forces de police alertées par l'événement, peuvent avoir été présents ou non lors de la commission de l'agression sexuelle (*Ver_Third*) ; ou le viol peut avoir été interrompu ou non pour une raison ou une autre (*Ver_Inte*). En ce qui concerne l'agresseur sexuel, on suppose qu'il a pu agir sous l'influence de l'alcool (*Ver_Alc*) ou de la drogue (*Ver_Drug*), voire que ses capacités volitives et intellectuelles ont été diminuées (*Ver_Vic*). Dans tous les cas détectés, les variables ont été codées 0 (absence du comportement), 1 (présence du comportement) ou 2 (comportement non mentionné dans la phrase).
- Le comportement sexuel de l'auteur de l'infraction. Les variables suivantes prennent trois valeurs possibles, 0 indiquant l'absence de comportement, 1 indiquant la présence d'un comportement et 2 indiquant un comportement non enregistré dans le dossier judiciaire. Les variables *Ver_Vag*, *Ver_Anal* et *Ver_Fel* indiquent que la victime a subi une pénétration avec le pénis dans le vagin, l'anus ou la bouche, respectivement. Les variables *Ver_Vag_Attempt* et *Ver_Anal_Attempt* indiquent que l'agresseur sexuel a tenté sans succès de pénétrer la victime avec son pénis dans le vagin ou l'anus, respectivement. La variable *Ver_Finger* indique que l'agresseur a pénétré la victime avec ses doigts dans le vagin ou l'anus.
- Comportements non sexuels de l'agresseur. Ces variables ont également pris les valeurs 0 (absence), 1 (présence) et 2 (pas d'enregistrement). Si l'agresseur a approché la victime au moyen d'une manœuvre trompeuse, la variable *Ver_Con* a été codée 1. Si l'agresseur a attaqué la victime par surprise, la variable *Ver_Surp* a été codée 1. S'il a utilisé une arme quelconque (généralement un couteau), la variable *Ver_Weap* a été codée 1. Si la victime s'est fait voler des objets de valeur (argent, téléphone portable, carte de crédit, etc.), la variable *Ver_Val* est codée 1. Si le vol concerne des objets personnels (sous-vêtements, photos, journal intime, etc.) susceptibles d'être utilisés à des fins fétichistes, la variable *Ver_Pers* est codée 1.
- Autres variables. Elles sont apparues en relation avec d'autres questions alternatives soulevées par les arrêts et qui présentent un intérêt pour l'analyse détaillée des affaires. Ainsi :
 - a. Le délinquant sexuel a-t-il fait preuve de connaissances médico-légales dans son comportement (utilisation de préservatifs, de gants, nettoyage, etc.) Si oui, la variable *Ver_Fore* a été codée à 1.
 - b. Le délinquant sexuel a-t-il agi entre 22 heures et 6 heures, heure locale ? Dans l'affirmative, la variable *Ver_Darkness* a été codée 1.

- c. L'auteur de l'infraction a-t-il agi entre un vendredi à midi et le lundi suivant à midi ? Si la réponse à cette question est positive, la variable *Ver_Wend* (week-end) est codée 1.

4. RÉSULTATS

Le tableau 1 montre le pourcentage de présence des variables décrites ci-dessus dans les condamnations pour agression sexuelle concernant les provinces de Madrid et de Barcelone. Comme le montre le tableau 2, deux variables présentent une différence significative entre Madrid et Barcelone, et une variable n'est pas significative, mais se situe à la limite de la signification $-p \leq 0,05$ -. On constate également que les délinquants sexuels agissent davantage sous l'influence de drogues et utilisent plus d'armes dans la province de Barcelone qu'à Madrid. Cependant, les pénétrations vaginales sont plus nombreuses dans les cas détectés à Madrid que dans ceux condamnés à Barcelone.

Tableau 1. Pourcentages de "présence" des différents comportements liés aux crimes analysés.

Variables	Signification	Madrid	Barcelone
Ag_Sex	Casier judiciaire de l'auteur d'infractions sexuelles.	5,3%	13,2%
Ag_Theft	Casier judiciaire de l'agresseur pour vol.	13,2%	13,2%
Ag_Viol	Le casier judiciaire de l'auteur de violences non sexuelles.	10,5%	10,5%
Ag_Unesp	Dossier judiciaire pour un délit non spécifié.	15,8%	15,8%
Ver_Resist	La victime a résisté.	52,6%	60,5%
Ver_Shout	La victime a crié.	23,7%	28,9%
Ver_Third	Des tiers alertés sont apparus.	31,6%	18,4%
Ver_Inte	L'agression sexuelle a été interrompue par des circonstances inattendues.	28,9%	34,2%
Ver_Alc	L'agresseur était sous l'influence de l'alcool.	5,3%	21,1%
Ver_Drug	L'agresseur était sous l'influence de drogues.	5,3%	28,9%
Ver_Vic	L'auteur avait des capacités volitives et intellectuelles réduites.	7,9%	18,4%
Ver_Vag	La victime a subi une pénétration vaginale.	76,3%	50,0%
Voir_Anal	La victime a subi une pénétration anale.	7,9%	15,8%
Ver_Fel	La victime a subi une pénétration orale (fellation).	34,2%	47,4%
Ver_Vag_Attemp	Une tentative de pénétration vaginale a échoué.	7,9%	13,2%
View_Anal_Attemp	Il y a eu une tentative de pénétration anale qui n'a pas abouti.	10,5%	10,5%
Ver_Finger	L'agresseur a pénétré la victime avec ses doigts dans le vagin ou l'anus.	13,2%	13,2%
Voir_Con	L'agresseur a approché la victime par la ruse.	55,3%	36,8%
Voir_Surp	L'agresseur s'est approché par surprise de la victime.	44,7%	63,2%
Ver_Weap	L'agresseur a utilisé une arme quelconque.	23,7%	47,4%
Ver_Vehi	L'agresseur s'est rendu sur les lieux de l'agression à bord d'un véhicule.	10,5%	5,3%
Ver_Val	L'agresseur a dérobé des actifs financiers à la victime.	36,8%	36,8%
Voir_Pers	L'agresseur a pris un objet pouvant être utilisé comme fétiche.	7,9%	5,3%
Ver_Fore	L'agresseur a fait preuve d'expertise médico-légale.	5,3%	15,8%

Ver_Darkness	L'agression a été commise entre 22 heures et 6 heures.	42,1%	39,5%
Ver_Wend	Le vol a été commis pendant le week-end (entre le vendredi midi et le lundi midi).	71,1%	60,5%

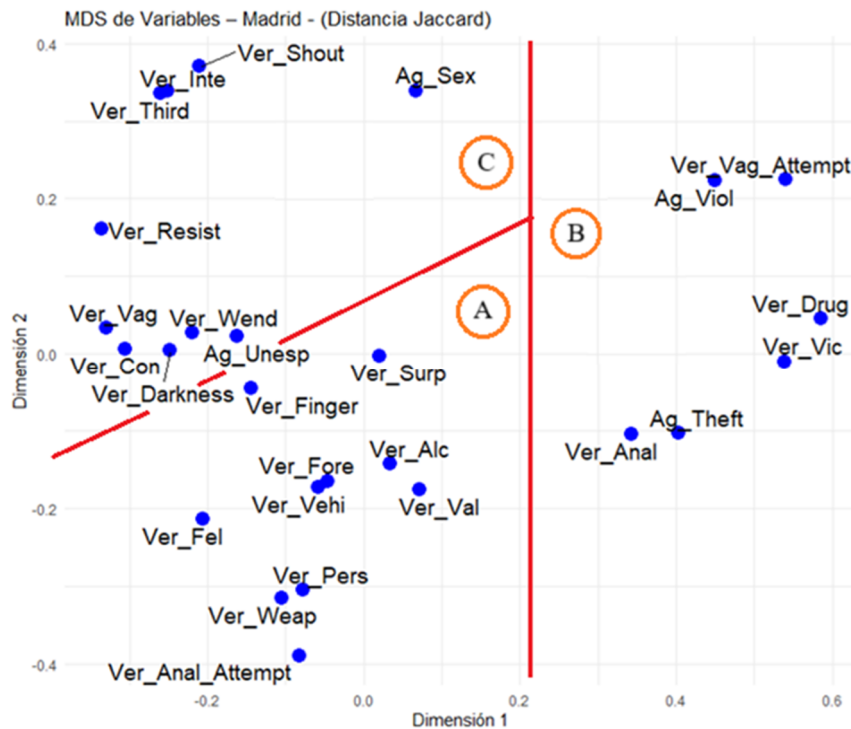
Tableau 2 : Variables qui ont montré des différences significatives entre les agressions sexuelles commises par des inconnus à Madrid et à Barcelone.

Variable	Valeur p	Test utilisé
Ver_Drug	0,012	Exact de Fisher
Ver_Vag	0,032	Khi-deux
Ver_Weap	0,055	Khi-deux

Le résultat de la procédure d'échelle multidimensionnelle (MDS) pour les cas madrilènes est visible dans la figure 1. Les 3 clusters trouvés (A, B et C, dans la figure), formés par les regroupements des données et qui déterminent autant de typologies, ont été trouvés au moyen de l'analyse de *clustering K-Means*. Les typologies détectées dans la province de Madrid, analysées indépendamment, seraient les suivantes :

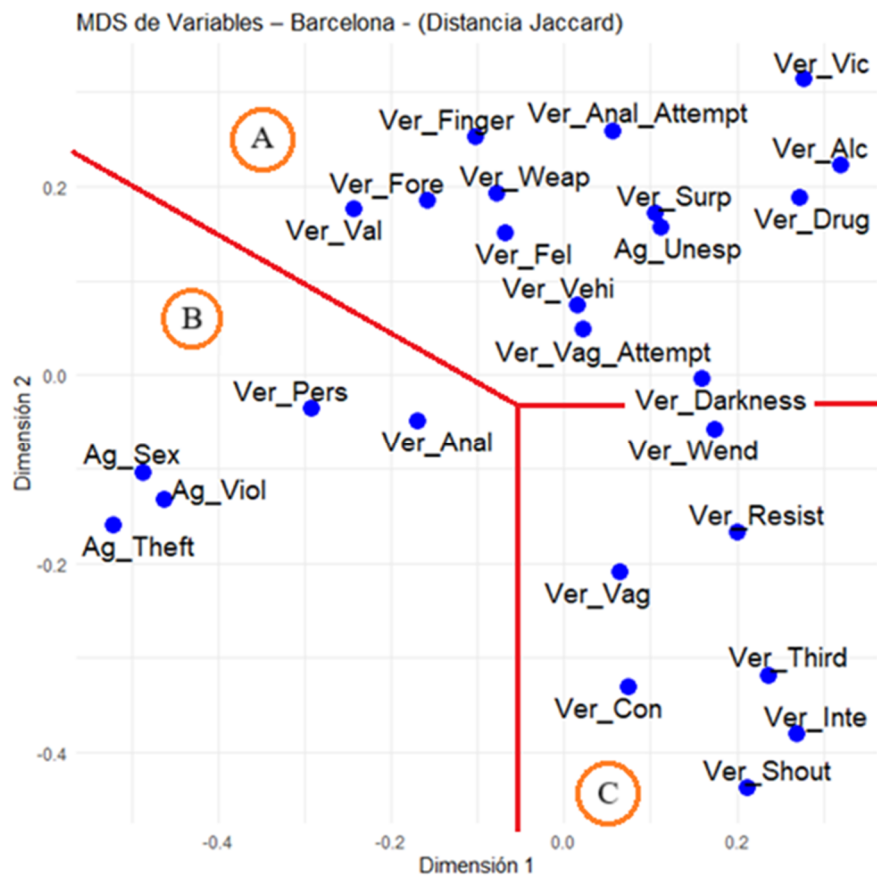
- Le type A, impulsif, est une personne ayant déjà commis d'autres agressions sexuelles, qui agit généralement dans l'obscurité, pendant le week-end, et s'approche de la victime en utilisant des subterfuges. Cependant, la victime résiste souvent et crie, alertant des tiers, de sorte que le viol, malgré l'existence d'une pénétration anale ou vaginale, est interrompu. Néanmoins, la victime peut être dépouillée de ses objets de valeur.
- Le type B, de nature polyvalente, montre un délinquant sexuel qui agit sous l'influence de drogues et dont les capacités intellectuelles et/ou volitives sont donc diminuées. Dans ce cas, où le délinquant peut avoir des antécédents de vol et d'autres crimes violents, il y a généralement une tentative infructueuse de pénétration vaginale, ainsi que de pénétration anale. On pourrait éventuellement penser à une personne dont le raisonnement est altéré, initialement motivée par le vol, qui tente de profiter de l'occasion.
- Le type C suggère la présence d'un agresseur sexuel planifié et plus spécialisé, doté d'une certaine connaissance de la médecine légale, qui se déplace dans un véhicule et qui utilise un type d'arme pendant l'agression afin d'intimider et de soumettre la volonté de ses victimes. Dans ce cas, l'agresseur consomme généralement de l'alcool et force la victime à lui faire une fellation, peut tenter une insertion vaginale avec ses doigts et une pénétration anale. Ce troisième type d'agresseur prélève généralement des objets sur la victime pour en faire des fétiches ou des trophées.

Figure 1 : Échelle multidimensionnelle des agressions sexuelles commises à Madrid.



Comme dans le cas précédent, les 3 clusters (A, B et C dans la figure), formés par les regroupements des données, ont été trouvés au moyen de l'analyse de *clustering K-Means*. Les typologies détectées dans la province de Barcelone sont les suivantes :

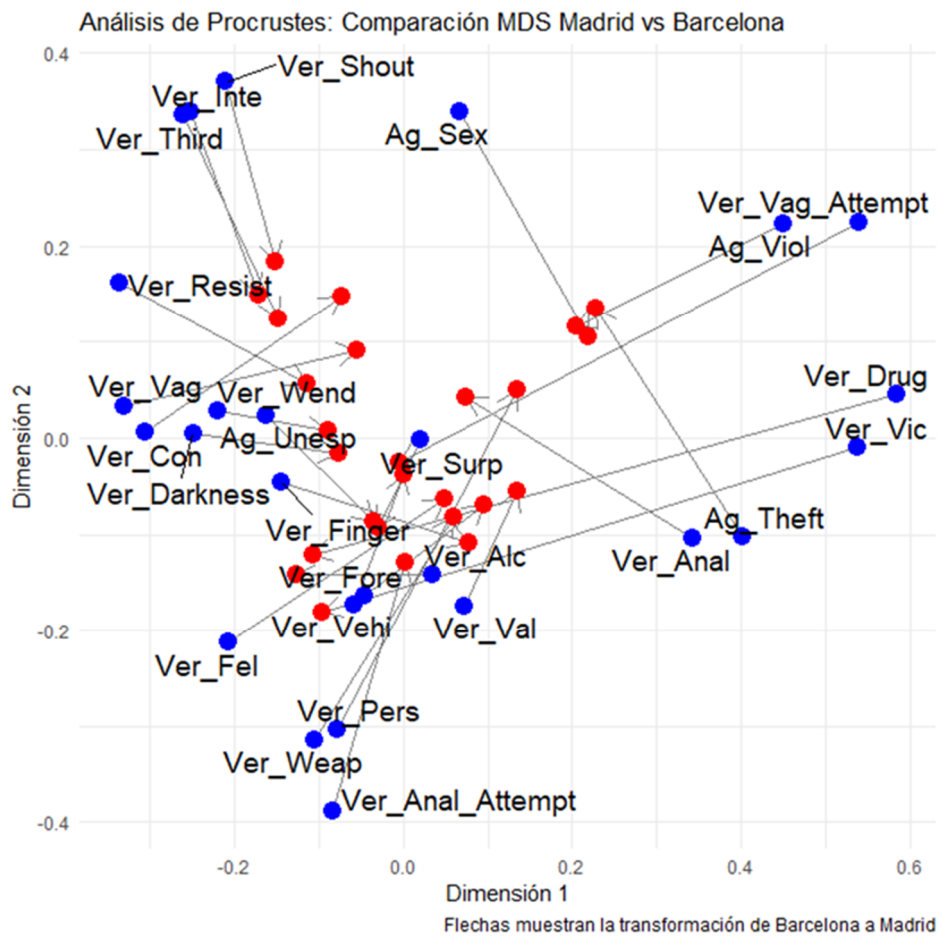
- Le type A, biais occasionnel, serait une personne ayant une certaine conscience médico-légale, qui se déplace en véhicule, consomme de la drogue et a des antécédents d'autres délits non spécifiés dans la peine. Cette personne, qui utilise souvent des armes pour maîtriser la victime et qui est sous l'influence de drogues et d'alcool, aborde ses victimes par surprise et peut essayer de les forcer à lui faire une fellation. Après avoir introduit ses doigts dans les parties génitales de la victime, et de manière indistincte, il tente de procéder à une pénétration anale et/ou vaginale, mais n'y parvient généralement pas.
- Le type B, très polyvalent, polycriminel et donc mal défini, est un délinquant ayant des antécédents d'autres délits sexuels, de vols et de violences non sexuelles, qui prélèvera sur la victime des objets sans valeur apparente pouvant être utilisés comme fétiches.
- Le type C, biais occasionnel et récréatif, opère la nuit et généralement le week-end. Il approche la victime par la tromperie et/ou divers subterfuges afin de procéder à la pénétration vaginale, mais en l'absence d'armes ou de planification préalable pour faciliter ses activités, la victime résistera, criera et alertera des tiers susceptibles d'interrompre l'agression.

Figure 2 : Échelle multidimensionnelle des agressions sexuelles commises à Barcelone.

Afin de comparer les agressions et les typologies présentes dans les deux contextes, le test de Procrustes a été appliqué aux échelles multidimensionnelles (MDS) qui montrent les clusters/typologies de Madrid et de Barcelone, de manière à obtenir la meilleure adéquation entre les deux. À l'issue de ce processus, l'indice de Jaccard (0,393) et l'indice ARI (0,332) ont été calculés. Il en résulte un chevauchement et une différenciation des typologies décrites pour chacun des contextes criminels. La figure 3 est le résultat du test de Procrustes visant à comparer le résultat du MDS appliqué aux données de Madrid avec le résultat du MDS appliqué aux données de Barcelone⁴. Il est important de souligner ici que l'analyse de Procrustes est utile pour évaluer la similarité entre deux configurations spatiales - ou nuages - de données. Les résultats obtenus par cette procédure montrent donc comment les configurations spatiales des données de Madrid et de Barcelone s'alignent après une transformation optimale (rotation, mise à l'échelle et translation) visant à minimiser autant que possible les différences entre elles.

⁴ L'analyse de Procrustes est un processus de transformation euclidienne dans la série des méthodes statistiques qui appliquent la théorie des groupes à l'analyse d'ensembles de données homogènes afin de les comparer entre eux et de faire des déductions à partir de ces comparaisons. C'est l'une des procédures incluses dans ce que l'on appelle "l'analyse statistique multivariée". Son nom vient du mythe de Procrustes, l'un des fils de Poséidon, qui était aussi un terrible tueur en série. Il possédait une maison où il hébergeait les voyageurs fatigués qui s'aventuraient dans la région. Il les invitait à s'allonger sur un lit de fer qu'il attachait, pendant leur sommeil, pieds et mains aux quatre coins. Si la victime propitiatoire est si grande que son corps dépasse le lit, Procrustes scie les parties saillantes de son corps. Si elle était plus courte que le lit, il la martelait pour l'étirer aux bonnes dimensions (Hurley et Cattell, 1962 ; Gower, 1975).

Figure 3 : Comparaison entre les DME des provinces de Madrid et de Barcelone.



4.1. TYPOLOGIES A

Dans le cas de Madrid, comme indiqué plus haut, ce groupe regroupe des variables liées à des délits où il y a vol d'objets ou une agression moins violente en termes physiques. À Barcelone, en revanche, on observe dans ce groupe une prédominance de délinquants ayant des antécédents de délits violents et de vols, sans variables indiquant directement une violence sexuelle consommée.

Les principales différences entre les deux environnements sont liées aux antécédents judiciaires, puisque dans le cas de Barcelone, il y a une forte présence de délinquants ayant des antécédents de délits sexuels, de vols et de violences. À Madrid, en revanche, le groupe est davantage lié au vol de biens matériels, de trophées ou de fétiches. Des variations significatives peuvent également être observées en ce qui concerne les agressions sexuelles proprement dites. Alors que dans les cas de la province de Barcelone, il y a une plus grande relation avec la pénétration anale, à Madrid, on observe des tentatives infructueuses de pénétration anale et des agressions avec les doigts ou la fellation.

En règle générale, on peut indiquer que dans le groupe A, pour Madrid, il y a plus de cas de tromperie, de subterfuge ou d'excuse pour approcher la victime et de vol, tandis

qu'à Barcelone, le casier judiciaire du délinquant devient un facteur clé à prendre en compte lors de l'évaluation de sa dangerosité potentielle.

4.2. TYPOLOGIES B

En ce qui concerne Madrid, les variables incluses dans ce groupe indiquent un profil d'agresseurs ayant un casier judiciaire pour des délits violents et/ou sexuels, ainsi que des circonstances dans lesquelles l'agresseur est sous l'influence de diverses substances. La victime, quant à elle, subit une agression sexuelle consommée ou une tentative d'agression sexuelle. En ce qui concerne Barcelone, les variables fournissent un profil d'agresseurs sans antécédents judiciaires spécifiques, mais avec des caractéristiques qui reflètent une planification claire de l'attaque et une consommation de substances.

Les principales différences en termes d'antécédents judiciaires sont que, pour Madrid, il y a une présence plus claire d'antécédents de vol et de violence, tandis qu'à Barcelone, il y a une catégorie plus ambiguë d'antécédents non spécifiés. En ce qui concerne le mode opératoire de l'agresseur, dans les cas de Barcelone, il y a plus de preuves de planification, comme le montre la présence très systématique de l'utilisation de la tromperie, de véhicules et d'armes. À Madrid, en revanche, la violence directe semble jouer un rôle beaucoup plus important.

En ce qui concerne la consommation de substances et l'agression sexuelle elle-même, on observe dans les deux cas la présence de drogues ou d'alcool, mais à Madrid, la violence sexuelle est plus évidente en termes d'agressions consommées. À Barcelone, dans le cadre du type B, on observe une plus grande tendance aux tentatives d'agression infructueuses, mais avec des méthodes plus diverses telles que la pénétration avec les doigts.

4.3. TYPOLOGIES C

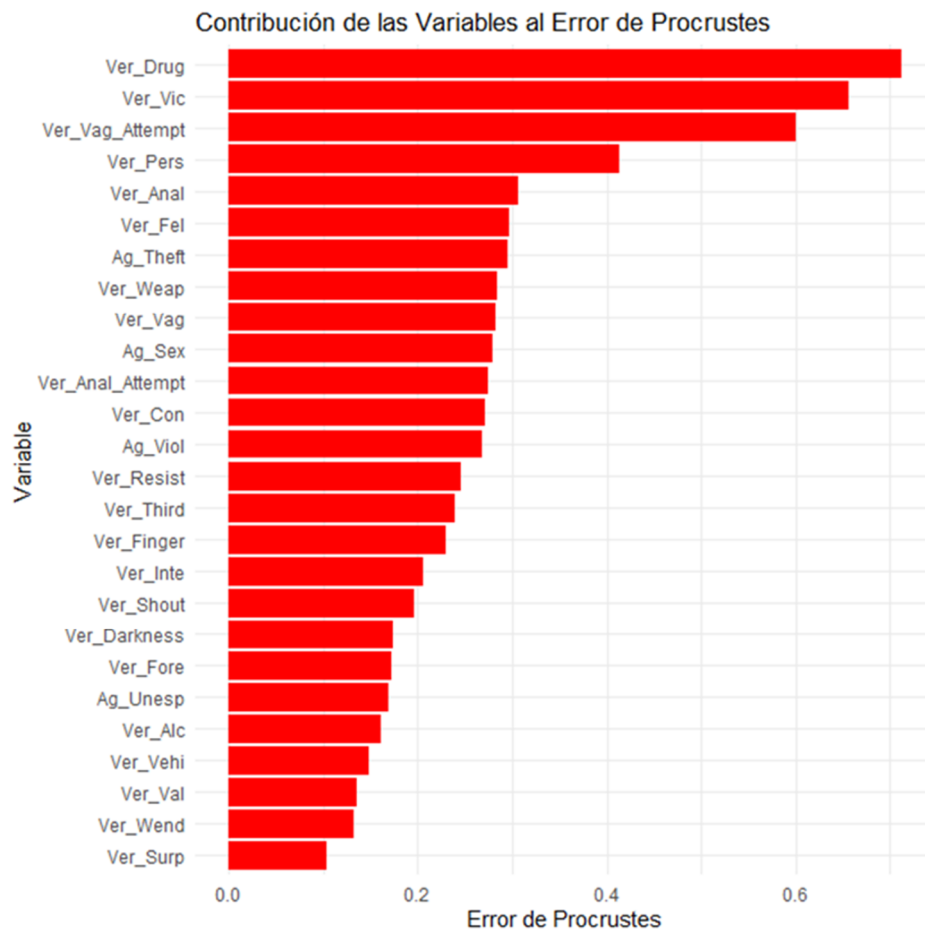
Dans le contexte de Madrid, les variables de ce groupe reflètent des agresseurs qui n'ont pas nécessairement un casier judiciaire grave, mais qui agissent de manière impulsive, sans grande planification et dans des environnements où la victime tente de résister et où il y a généralement l'intervention d'une tierce personne. Dans le cas de Barcelone, on trouve également des agressions interrompues, mais qui mettent moins l'accent sur l'utilisation de la tromperie pour approcher la victime et sur l'intervention de tiers qui peuvent contrecarrer l'agression.

Les principales différences, en ce qui concerne les antécédents judiciaires, sont liées à Madrid au fait que ce groupe comprend des agresseurs ayant des antécédents de délits sexuels, alors qu'à Barcelone, il n'est pas fait mention de tels antécédents. Comme nous l'avons déjà mentionné, dans les deux cas, il y a une résistance de la part de la victime et une éventuelle interruption de l'agression, mais à Madrid, il y a plus de variables associées à la présence de tiers. De même, dans les agressions commises dans la province de Madrid, la nuit est un facteur plus important, alors qu'à Barcelone, la variable de la nuit n'apparaît pas dans ce groupe.

La figure 4, quant à elle, est illustrative en ce sens qu'elle représente la contribution de chaque variable à l'erreur de Procrustes, c'est-à-dire à la non-concordance des deux ensembles de données. Elle indique quels aspects de l'agression diffèrent le plus entre les

configurations de données trouvées entre les groupes de Madrid et de Barcelone après transformation.

Figure 4 : Différences de chacune des variables dans la position spatiale du MDS obtenu avec les données de Madrid et de Barcelone.



Plusieurs éléments doivent être pris en compte dans l'interprétation générale des résultats décrits ci-dessus :

1. Nombre d'objets et de dimensions : 26 variables ont été comparées dans un espace bidimensionnel.
2. Mesure d'adéquation (somme des carrés de Procrustes) : 2,6286, indique le niveau de différence entre les configurations avant et après la transformation.
3. L'erreur quadratique moyenne de Procrustes (RMSE) : 0,31796, représente l'ampleur moyenne de l'erreur dans l'alignement des points (tableau 3).

Distribution des erreurs quadratiques moyennes trouvées dans l'analyse de Procrustes.

Erreur minimale	0,1041
Premier quartile (Q1)	0,1719
Moyen	0,2568
Troisième quartile (Q3)	0,2919
Erreur maximale	0,7121

Compte tenu de tout ce qui précède, les données du tableau 3 suggèrent que la plupart des variables ont une erreur d'ajustement relativement faible, mais que certaines ont des erreurs plus élevées. En tout état de cause, pour obtenir le meilleur ajustement possible des graphiques présentés dans les figures 1 et 2, il a fallu effectuer une rotation de 180°, avec une translation pratiquement nulle et une mise à l'échelle d'environ 0,5. Cela n'a pas impliqué une altération significative des résultats et a répondu au fait que le graphique de la province de Barcelone avait une taille linéaire d'environ la moitié de celle obtenue avec les données de la province de Madrid, ce qui a empêché d'effectuer des comparaisons adéquates. Le fait est que les configurations de Madrid et de Barcelone sont similaires en termes de structure, mais différentes en termes d'échelle et d'orientation. Cela indique en soi qu'il existe des différences entre les données des deux provinces qui ne peuvent être ignorées et que, par conséquent, nous avons affaire à des réalités différentes par rapport à l'objet de l'étude. Ainsi, bien que la correspondance entre les ensembles de données soit acceptable, certains items présentent des erreurs plus élevées qui indiquent des différences dans la façon dont certains types d'agression - et les comportements des délinquants - sont structurés dans les deux provinces.

Une fois cette précision apportée, un examen plus approfondi de la figure 3 montre que les points bleus représentent la configuration originale de Madrid avant la transformation, tandis que les points rouges représentent la configuration transformée de Barcelone afin de s'aligner sur celle de Madrid. Les flèches indiquent l'ampleur et la direction de l'ajustement nécessaire pour aligner Barcelone sur Madrid. Comme le montrent les résultats numériques, la structure de Barcelone a subi une rotation de près de 180°, ainsi qu'une mise à l'échelle par rapport à la procédure de Procrustes, afin de l'aligner sur celle de Madrid. Cela est évident car certains points bleus et rouges se trouvent dans des positions opposées dans certaines zones. Les points dont les lignes sont plus longues et qui se rapportent à la même variable indiquent qu'il existe des différences significatives dans la représentation de cette variable entre les deux villes. Par exemple, *Ver_Drug*, *Ver_Vic* et *Ver_Vag_Attempt* montrent des décalages importants, ce qui suggère que la représentation spatiale de Madrid dans le MDS est différente de celle de Barcelone.

D'autre part, dans les zones où la concordance est la plus élevée, c'est-à-dire là où les variables où les points rouges et bleus sont proches, des structures similaires sont suggérées dans les deux provinces. Par exemple, *Ver_Finger*, *Ver_Fore* et *Ver_Alc* présentent moins de déplacements, ce qui indique que leurs structures sont similaires dans les deux villes. La structure générale des types d'agressions et des comportements qui y sont liés est similaire dans les deux villes, mais avec des différences intéressantes en termes d'orientation et d'échelle. Comme nous l'avons déjà vu, certaines variables présentent une plus grande divergence, comme dans les cas de *Ver_Drug*, *Ver_Vic* et *Ver_Vag_Attempt*, ce qui indique que ces facteurs sont perçus ou structurés différemment dans chaque province. D'autres variables ont des structures similaires, suggérant des modèles communs d'agression et de réponse dans les deux villes que la criminologie devrait expliquer afin d'approfondir son champ de recherche et ne pas se contenter de supposer.

De telles différences dans les structures des MDS correspondants de Madrid et de Barcelone doivent nécessairement être liées aux typologies trouvées par la procédure *K-Means*. Reportez-vous maintenant à la figure 4, qui vous aidera à clarifier numériquement

ce qui se passe. Les variables présentant l'erreur de Procrustes la plus élevée - c'est-à-dire celles qui diffèrent le plus entre les deux villes - sont les suivantes :

- *Ver_Drug* (0.71) : L'auteur de l'infraction était sous l'influence de drogues.
- *Ver_Vic* (0.66) : Les capacités volitives et intellectuelles du délinquant sont altérées.
- *Ver_Vag_Attempt* (0.60) : La tentative de pénétration vaginale a échoué.
- *Ver_Pers* (0,41) : L'auteur a volé un objet pouvant être utilisé comme fétiche.
- *Ver_Anal* (0,30) : La victime a subi une pénétration anale.
- *Ver_Fel* (0,29) : La victime a subi une pénétration orale (fellation).
- *Ag_Theft* (0,29) : Dossier judiciaire du délinquant pour vol.
- *Ver_Weap* (0.28) : L'agresseur a utilisé une arme quelconque. Il existe des différences dans les agressions où l'agresseur utilise une arme, plus fréquentes à Barcelone.
- *Ver_Vag* (0,28) : La victime a subi une pénétration vaginale.

5. DISCUSSION

Il semble évident que l'étude comparative entre les agressions sexuelles commises par des étrangers dans les provinces de Madrid et de Barcelone a révélé des différences significatives dans la manière dont ces crimes sont perpétrés dans chacun des contextes et que, par conséquent, l'hypothèse initiale est remplie. L'analyse de 76 cas extraits de décisions judiciaires et examinés à l'aide de tests statistiques robustes - test exact de Fisher, chi-carré, échelle multidimensionnelle et analyse de Procrustes - a permis d'identifier des schémas distinctifs dans les agressions sexuelles commises dans les deux territoires.

En ce qui concerne la pertinence des statistiques utilisées, l'utilisation du test exact de Fisher et du chi-carré pour comparer la présence de certaines caractéristiques dans les crimes commis à Madrid et à Barcelone a permis d'établir des différences significatives - ou presque - sur des aspects clés tels que la consommation de drogues par l'agresseur (*Ver_Drug*, $p = 0,012$), l'utilisation d'armes (*Ver_Weap*, $p = 0,055$, à la limite de la significativité) et la pénétration vaginale (*Ver_Vag*, $p = 0,032$). Ces tests étaient appropriés pour évaluer les associations entre des variables catégorielles dans un ensemble de données représentatif mais relativement petit.

Les analyses MDS et *K-means* ont permis d'identifier des typologies de délinquants et des modèles d'agression dans chaque province, montrant des différences structurelles dans la façon dont ces crimes sont commis. L'analyse Procrustes a montré - toujours dans le cadre de l'échantillon de référence, ce qui doit inciter à une prudence raisonnable - que, bien que la structure des agressions sexuelles soit similaire dans les deux régions, l'échelle et l'orientation des facteurs diffèrent de manière significative, indiquant des schémas spécifiques dans chaque région.

En ce qui concerne les différences entre Madrid et Barcelone, l'analyse statistique et spatiale des données a révélé que, bien que les crimes sexuels commis par des étrangers présentent des similitudes structurelles à Madrid et à Barcelone, il existe des différences importantes dans les méthodes et les circonstances des agressions, ce qui souligne

l'importance d'une étude détaillée des deux écosystèmes criminels, comme mentionné dans l'introduction, et comme prévu par le TAS :

- Une plus grande consommation de drogues par les délinquants à Barcelone : 28,9% des délinquants étaient sous l'influence de drogues au moment de l'infraction, contre seulement 5,3% à Madrid. Cela pourrait indiquer une plus grande association entre la consommation de substances et l'agression à Barcelone ou un contexte criminologique différent dans lequel les délinquants de Barcelone ont plus d'antécédents de consommation de drogues au moment de l'agression.
- Une plus grande utilisation d'armes dans la province de Barcelone : 47,4% des agresseurs ont utilisé un type d'arme pour maîtriser la victime, alors qu'à Madrid ce pourcentage est de 23,7%. Cela suggère un degré plus élevé de violence instrumentale dans les agressions commises à Barcelone, qui pourrait être lié à des facteurs environnementaux ou criminologiques spécifiques au contexte.
- Différences dans la manière de perpétrer l'agression sexuelle : à Madrid, la pénétration vaginale était plus fréquente (76,3%) qu'à Barcelone (50%). En revanche, les agressions avec pénétration orale (fellation) sont plus fréquentes à Barcelone (47,4%) qu'à Madrid (34,2%). De même, la pénétration anale était également plus fréquente à Barcelone (15,8%) qu'à Madrid (7,9%).
- Différences dans la stratégie d'approche de l'agresseur : à Madrid, les agresseurs ont utilisé davantage de stratégies de tromperie, de distraction ou de subterfuge pour approcher la victime (55,3 %) qu'à Barcelone (36,8 %). En revanche, un plus grand nombre d'attaques surprises et non planifiées ont été observées à Barcelone (63,2 % contre 44,7 % à Madrid). Cela suggère que les agresseurs de la province de Barcelone optent plus fréquemment pour des attaques directes et violentes, tandis que ceux de Madrid recourent davantage à la manipulation et à la tromperie pour réduire la résistance de la victime potentielle.
- Différences dans la réaction de la victime et l'interruption de l'acte criminel : les victimes de Barcelone ont eu tendance à résister dans une plus grande proportion (60,5 %) que celles de Madrid (52,6 %). C'est peut-être pour cette raison que l'interruption de l'agression en raison de circonstances inattendues a été plus fréquente à Barcelone (34,2%) qu'à Madrid (28,9%), ce qui suggère qu'à Barcelone les agressions ont eu tendance à se produire dans des contextes moins contrôlés par l'agresseur, ce qui est logique compte tenu de l'idée d'un plus grand recours à la violence et, par conséquent, d'une composante de plus grande impulsivité et d'un contrôle moins pratique de la scène chez l'agresseur sexuel inconnu dans la province de Barcelone.
- Casier judiciaire du délinquant : les délinquants de Barcelone avaient un nombre plus élevé de casiers judiciaires pour des délits sexuels antérieurs (13,2%) que ceux de Madrid (5,3%). Il n'y avait cependant pas de différences significatives dans les casiers judiciaires pour vol ou violence non sexuelle.

6. CONCLUSIONS

A partir des résultats décrits dans cette étude, il est possible de décrire un profil des agressions sexuelles par des inconnus que l'on retrouve dans les condamnations prononcées dans chacune des provinces analysées.

À Madrid, la tromperie pour approcher la victime est plus fréquente, la pénétration vaginale plus fréquente, l'utilisation d'armes et de drogues au moment de l'agression plus faible et le groupe d'agresseurs ayant moins de condamnations antérieures pour des délits sexuels. À Barcelone, en revanche, les attaques surprises sont plus fréquentes, l'utilisation d'armes et de drogues est plus importante et le nombre d'auteurs ayant un casier judiciaire pour des délits sexuels est plus élevé. Une fréquence plus élevée d'agressions avec pénétration orale et anale a également été détectée, ainsi qu'une plus grande tendance de la victime à résister, bien que la proportion d'agressions interrompues par des facteurs externes soit plus élevée.

Les résultats de cette étude confirment que les agressions sexuelles perpétrées par des inconnus présentent des différences significatives dans les deux territoires, ce qui suggère la nécessité de stratégies de prévention et de réponse adaptées aux caractéristiques criminologiques spécifiques de chaque ville. Ceci, dans le cadre du TAS, ne serait possible qu'en prêtant attention à une analyse détaillée du contexte délinquant-criminel dans lequel les agresseurs agissent dans chaque cas, ce qui nécessiterait des études concrètes, spécifiques, détaillées et circonstanciées qui, tout simplement, remettent en cause la validité du TAS, remettent en cause la validité des grandes théories et méthodologies - qui expliquent le général avec certaines garanties, mais tendent à échouer dans leur approche du particulier - et imposent la nécessité d'une étude chirurgicale de chaque écosystème criminel afin de définir des politiques précises et efficaces - de détection, d'investigation et de prévention. Ainsi, par exemple, ce travail suggère que dans la province de Barcelone, étant donné l'utilisation plus importante d'armes et de drogues dans les attentats, il conviendrait de mettre en œuvre les mesures de contrôle pertinentes sur ces aspects, ainsi que de procéder à une étude plus approfondie, détaillée et précise de l'histoire criminelle des agresseurs potentiels. À Madrid, cependant, la tendance marquée à l'utilisation de la tromperie dans l'approche de la victime potentielle par l'agresseur sexuel pourrait indiquer la nécessité de campagnes de sensibilisation pour aider les femmes à identifier l'utilisation d'éventuelles stratégies de manipulation, de contrôle et d'isolement chez les inconnus.

D'un point de vue criminologique, et toujours en tenant compte des variables écosystémiques, les résultats soulignent l'importance d'une recherche plus approfondie sur la relation entre le passé criminel - leur carrière criminelle antérieure, en général - des agresseurs et leur comportement pendant l'agression, ainsi que les différences détectables dans la réponse spécifique des victimes et les facteurs qui peuvent conduire à l'interruption d'une attaque, ce qui peut suggérer des avancées et des développements intéressants dans le cadre des politiques pénales au niveau régional et même provincial.

D'autre part, il convient de noter l'importance de cette étude pour le développement de techniques criminologiques auxiliaires à l'enquête policière, et plus particulièrement pour la croissance du profilage criminologique inductif - analyse comportementale -, car les données trouvées sont utiles pour la qualification détaillée des typologies criminelles actuelles qui, souvent, parce qu'elles sont excessivement larges,

tendent à être peu utiles en termes d'application pratique. Nous constatons, par exemple, que dans la province de Madrid, les agresseurs présentent des groupes plus différenciés en fonction de la gravité du délit commis, tandis que dans la province de Barcelone, l'agresseur présente une organisation comportementale plus liée à son histoire criminelle spécifique. Dans les deux cas, indistinctement, la consommation de substances et la planification de l'attaque jouent un rôle important, mais il existe des différences claires en termes d'exécution et d'interruption du crime qui devraient être connues et correctement nuancées, car elles seraient d'une grande aide en termes de conception de profils criminels spécifiques, ainsi que dans les processus d'enquête policière.

En fin de compte, cette étude, qui ne porte que sur deux provinces, mais qui pourrait être étendue à l'échelle nationale avec un financement et une infrastructure adéquats, contribue à une meilleure compréhension de la violence sexuelle entre inconnus, tout en montrant qu'une étude situationnelle-écologique de la criminalité fournit non seulement des données utiles pour améliorer la prévention, l'intervention et les poursuites en matière de criminalité, mais qu'elle permet également de dépasser les généralités en matière de compréhension criminologique.

7. RÉFÉRENCES BIBLIOGRAPHIQUES

- Arqué-Valle, P., Pastor-Cárcel, A., Roca-Mercadé, C. et Soria M.A. (2024). Cultural influence on the sexual motivation of serial killers. *Logos Science & Technology Journal*, 16(1), 145-159, doi : <https://doi.org/10.22335/rlct.v16i1.1908>
- CGPJ (2023). Les tribunaux ont accordé 1 205 réductions de peine en application de la loi organique 10/2022 [disponible à l'adresse : <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/En-Portada/Los-tribunales-han-acordado-1-205-reducciones-de-pena-en-aplicacion-de-la-Ley-Organica-10-2022> , recueillie en mars 2024].
- Corovic, J., Christianson, S.A. et Bergman, R. (2012). From crime scene actions in stranger rape to prediction of rapist type : single victim or serial rapist ? *Behavioral Science and the Law*, 30, 764-781.
- Domínguez Vela, M. (2016). Violence de genre et victimisation secondaire. *Journal numérique de médecine psychosomatique et de psychothérapie*, Vol. 6(1). [disponible à l'adresse : https://www.psicociencias.org/pdf_noticias/Violencia_de_geneo_y_victimizacion_secundaria.pdf , récupéré en mai 2024].
- Gower, J.C. (1975). Generalized Procrustes analysis. *Psychometrika*, 40, 33-51.
- Gutiérrez de Piñeres Botero, C., Coronel, E. et Pérez, C.A. (2009). Examen théorique du concept de victimisation secondaire. *Liberabit* [en ligne], 15(1), 49-58 [disponible à l'adresse : https://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1729-48272009000100006 , récupéré en mars 2024].
- Hurley, J. R., et Cattell, R. B. (1962). The Procrustes Program : Producing direct rotation to test a hypothesized factor structure. *Behavioral Science*, 7(2), 258-262. <https://doi.org/10.1002/bs.3830070216>
- Janosch González, H. (2013). Les fondements philosophiques de la criminologie chez Hirschi et Wikström : Popper ou Bunge ? In Serrano Maíllo, A., et Birkbeck, C., (Eds.) *The Generality of Self-Control Theory. Une première extension de la théorie générale du crime aux pays hispanophones*. Madrid : Editorial Dykinson.
- Janosch, H., Pérez-Fernández, F., Nut, D. et Marset, M. (2023). Agresseurs sexuels inconnus de la victime en Espagne. A multidimensional scaling analysis (MDE) based on an analysis of sentences. *Revista de Derecho Penal y Criminología*, 3^a Época, 30, 395-411.
- Janosch, H., Pérez-Fernández, F. et Herrero, S. (2025). Agresseurs sexuels inconnus de la victime dans la Communauté de Madrid : une analyse exploratoire des peines prononcées par l'Audience Provinciale. H. Janosch et F. Pérez-Fernández (coords.), *Panorámica de los delitos sexuales en España*. Madrid : Dykinson, 43-85.

- Janosch, H., Pérez-Fernández, F. et Popiuc, M. (2023). Low self-control in non-heterosexual men as a predictor of sexual assault behaviors against women. *Behavior & Law Journal*, 9(1), 65-79, <https://doi.org/10.47442/blj.2023.100>
- Janosch, H., Pérez-Fernández, F., Popiuc, M. et López-Muñoz F. (2024). Relationship between low personal morality and impersonal sex with sexual aggression behaviors towards women in a sample of Spanish heterosexual men", *Journal of Asia Pacific Studies*, 7(2), 109-139.
- Janosch González, H., Pérez-Fernández, F. et Soto Castro, J.E. (2020). Un modèle de profilage pour les délinquants sexuels inconnus qui agressent à l'entrée des bâtiments. *Revista de Derecho Penal y Criminología*, 3^a época, 24, 243-258.
- Kühne, H.H. (1986). *Kriminologie : Victimologie der Notzucht*", *Juristische Schulung*, 5, 388-394.
- Linde, A. et Aebi, M.F. (2021). Does theft really mean theft ? and other dubious equivalences between legal and criminological definitions of offences. Conséquences pour l'étude de la criminalité. *Revista Española de Investigación Criminológica*, 19, Extra-2 [www.criminologia.net], <https://doi.org/10.46381/reic.v19i2.529> .
- Ministère espagnol de l'intérieur (2023). *Annuaire statistique du ministère de l'intérieur 2022. Catalogue des publications de l'administration générale de l'État :* <https://cpage.mpr.gob.es>
- Pauwels, L., 2018a. Analyse du processus de perception-choix dans la théorie de l'action situationnelle. A randomized scenario study. *European Journal of Criminology*, 19(1), 130-147.
- Pauwels, L. (2018b). Les effets conditionnels du contrôle de soi dans la théorie de l'action situationnelle. Un test préliminaire dans une étude de scénario randomisé. *Deviant Behavior*.
- Pérez-Fernández, F., Janosch, H. et Popiuc, M. (2023). Low self-control in non-heterosexual men as a predictor of sexual assault behaviors against women. *Behavior & Law Journal*, 9(1), 65-79. <https://doi.org/10.47442/blj.2023.100>
- Pueyo, A.A. et Redondo Illescas, S. (2007). Prédire la violence. Entre la dangerosité et l'évaluation du risque de violence. *Papeles del Psicólogo*, 28(3), 157-173.
- Serrano Maíllo, A. (2017). *Criminalité, moralité individuelle et contrôles*. Valence : Tirant Lo Blanch.
- Triviño, C., Winberg, M. et Moral, M. (2021). Credibility of Testimony in Child Sexual Assault and Abuse : Evolution of Non-Believable Testimony in the Last Decade. *Behavior & Law Journal*, 7(1), 43-57. <https://doi.org/10.47442/blj.v7.i1.83>

- Wikström, P.-O., Oberwittler, D., Treiber, K. et Hardie, B. (2012). *Breaking Rules : The Social and Situational Dynamics of Young People's Urban Crime*. Oxford : Oxford University Press.
- Wikström, P.-O. et Treiber, K. (2016). Social Disadvantage and Crime : A Criminological Puzzle (Désavantage social et criminalité : un casse-tête criminologique). *American Behavioral Scientist* 60(10), 1232-1259.



Article de recherche

DROGUES ET CONDUITE: "TOLÉRANCE ZÉRO" MÉTHODOLOGIE DU RAPPORT SALIVAIRE SYNLAB ET CRITÈRES D'APPROBATION DE L'ORGANISME NATIONAL D'ACCRÉDITATION

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

Juan Carlos Rodríguez Bello
Caporal 1 de la Guardia Civil
Groupement de circulation de la Guardia Civil
Expert universitaire en criminalité routière de l'UNED (UNED)
Expert judiciaire en contrôle documentaire par l'UNED (UNED)
jcrbello@guardiacivil.es

Reçu le 18/02/2025
Accepté le 14/05/2025
Publié le 27/06/2025

Citation recommandée : Rodríguez, J. C. (2025). Drogues et conduite : méthodologie "tolérance zéro" du rapport salivaire du laboratoire Synlab et critères d'homologation de l'entité nationale d'accréditation. *Revista Logos Guardia Civil*, 3(2), p.p. 197-220.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

DROGUES ET CONDUITE : "TOLÉRANCE ZÉRO" MÉTHODOLOGIE DU RAPPORT SALIVAIRE SYNLAB ET CRITÈRES D'APPROBATION DE L'ORGANISME NATIONAL D'ACCRÉDITATION

Résumé: INTRODUCTION. 2. STRATÉGIE DE LA DIRECTION GÉNÉRALE DE LA CIRCULATION : "TOLÉRANCE ZÉRO". 2.1. RAISON D'ÊTRE ET PROCÉDURE DE RÉALISATION DES TESTS SALIVAIRES DE DÉPISTAGE DE DROGUES. 3. LA DOCTRINE DU PARQUET GÉNÉRAL DE L'ÉTAT APRÈS LE TEST SALIVAIRE "POSITIF" AUX DROGUES. 4. LA PRÉSENCE DE DROGUES DANS L'ORGANISME : LA SANCTION ADMINISTRATIVE ET LA DOCTRINE DE LA COUR CONSTITUTIONNELLE. 5. LES "CUT-OFF POINTS" ET LES QUANTITÉS PSYCHOACTIVES MINIMALES. 6. LA SOCIÉTÉ D'ANALYSE CLINIQUE SYNLAB. 7. LES LIMITES DE QUANTIFICATION ET LES PLAGES D'INCERTITUDE DU LABORATOIRE SYNLAB. 8. LE LABORATOIRE SYNLAB ET SON ACCRÉDITATION PAR L'ORGANISME NATIONAL D'ACCRÉDITATION PAR LE BIAIS D'AUDITS. 9. PORTÉE DE L'ACCRÉDITATION ENAC 1169/LE2347 DÉLIVRÉE AUX LABORATOIRES SYNLAB. 10. CONCLUSIONS. 11. BIBLIOGRAPHIE. 10. CONCLUSIONS. 11. RÉFÉRENCES BIBLIOGRAPHIQUES. ANNEXE I - COMPOSITION ET PRINCIPES DU DED (ANALYSEUR) SOTOXA.

Résumé : La législation sur le contrôle de la consommation d'alcool et de drogues a un impact important sur la société, pas toujours sans controverse, selon la manière dont ces informations sont transmises à l'opinion publique. Les critères utilisés pour établir la limite légale de consommation d'alcool compatible avec la conduite d'un véhicule en sont un bon exemple. Bien que la société accepte le critère de tolérance zéro pour la consommation de drogues, il est essentiel de normaliser les méthodes utilisées pour détecter et quantifier la présence de drogues qui influencent la conduite et, par conséquent, la sécurité routière. Dans ce contexte, l'établissement et la détermination de la quantité des concentrations minimales, en cas de test de drogue positif, sont essentiels et particulièrement importants dans le cas des récidivistes ou des délinquants de la route. Toutefois, cette détermination qualitative et quantitative doit faire l'objet d'un contrôle approprié. Cet article rappelle l'histoire qui a conduit à la détermination des quantités détectables de drogues, mais surtout les critères de traçabilité qui caractérisent les systèmes accrédités dans le domaine de la Sécurité Routière.

Resumen: La legislación sobre el control del consumo de alcohol y drogas tiene una gran repercusión en la sociedad, no siempre exenta de polémica, dependiendo de cómo se traslade esta información a la opinión pública. Un claro ejemplo, lo tenemos con los criterios que se utilizan para establecer el límite legal de consumo de alcohol compatible con la conducción. Si bien es aceptado por la sociedad el criterio de tolerancia cero en cuanto al consumo de drogas, es fundamental la estandarización de los métodos por los que se detecta y cuantifica la presencia de drogas que influye en la conducción y, consecuentemente, afecta a la Seguridad Vial. En este contexto, establecer y determinar la cantidad de las concentraciones mínimas, en caso de detectarse un positivo en drogas, es imprescindible y especialmente importante en conductores reincidentes o en los delincuentes viales. Sin embargo, esta determinación cualitativa y cuantitativa debe estar debidamente auditada. En este artículo, se hace una revisión del histórico que ha llevado a la determinación de las cantidades detectables de drogas, pero, sobre todo, a los criterios de trazabilidad que son propios de sistemas acreditados en el ámbito de la Seguridad Vial.

Mots-clés : Sécurité routière, tolérance zéro, conduite, drogues, détection, concentration minimale, normalisation, accréditation

Palabras clave: Seguridad Vial, tolerancia cero, conducción, drogas, detección, concentración mínima, estandarización, acreditación.

ABBREVIATIONS

Art. 2 : Article.

PC : Code pénal.

DED : Dispositif de détection électronique (drogue portable).

DGT : Dirección General de Tráfico.

ENAC : Entidad Nacional de Acreditación (Entité nationale d'accréditation)

FSCSV : Procureur de la Chambre de coordination de la sécurité routière

FGE : Fiscalía General del Estado.

ISO : Organisation internationale de standardisation (norme internationalement reconnue).

LOQ : Limite de quantification.

LSV : Loi sur la sécurité routière.

Ng : nanogramme (1ng = 1,0E-9 g).

SV : Sécurité routière.

OMS : Organisation mondiale de la santé.

ONSV : Observatoire national de la sécurité routière.

ONU : Nations unies.

SV : Sécurité routière.

TC : Cour constitutionnelle.

UNE : Une norme espagnole.

UE : Union européenne.

1. INTRODUCTION.

Dans le "Plan mondial - Décennie d'action pour la sécurité routière¹ 2021-2030" de l'Organisation mondiale de la santé (OMS-ONU), il a été établi que l'un des principaux comportements contribuant aux décès et aux victimes des accidents de la route est la conduite en état d'ébriété. L'OMS invite donc les gouvernements à concevoir un système de transport routier sûr en adoptant des lois sur la sécurité routière, à faire appliquer ces lois et à promouvoir l'éducation routière. En outre, l'organisme onusien exhorte non seulement les organismes officiels, mais aussi les entreprises privées à prendre des mesures pour atténuer les effets négatifs sur la sécurité routière et à faire passer le message qu'une forte consommation d'alcool et d'autres substances, telles que les drogues, contribue à une "conduite dangereuse". L'OMS fixe également deux objectifs pour 2030 : réduire de moitié le nombre de décès et de victimes d'accidents de la route causés par des conducteurs sous l'emprise de l'alcool et réduire le nombre d'accidents causés par la consommation de substances psychoactives.

En Espagne, l'Observatoire national de la sécurité routière (ONSV)², organisme dépendant du ministère de l'Intérieur et géré par la Direction générale du trafic (DGT), a publié une "Revue systématique sur les drogues et la conduite (2021)". Ce document fait référence à la "Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial" (LSV)³, et plus particulièrement à l'article 14, qui interdit la conduite en présence⁴ de drogues dans le corps (à l'exclusion des substances utilisées sur prescription médicale et à des fins thérapeutiques). Toutefois, dans cette section de la LSV, le législateur avertit que "(...) à condition que (le conducteur) soit capable d'utiliser le véhicule conformément à l'obligation de diligence, de prudence et de non-distraction⁵ établie à l'article 10".

En outre, en Espagne, la conduite d'un véhicule à moteur "sous l'influence de drogues toxiques, de stupéfiants ou de substances psychotropes" peut constituer un délit contre la SV, tel que défini à l'article 379.2 de la loi organique 10/2015 du code pénal (CP). C'est pourquoi, le 17 juillet 2019, le parquet général de l'État (FGE), par l'intermédiaire du parquet de coordination de la sécurité routière (FSCSV), a publié une instruction pour la préparation des attestations relatives aux infractions de conduite sous l'influence de drogues toxiques, de stupéfiants et de substances psychotropes de l'article 379.2 du code pénal. Dans cette instruction, l'accent est mis sur l'importance du rapport des signes extérieurs pour déterminer l'influence de ces substances, étant donné que le législateur espagnol ne disposait pas d'un taux objectif pour déterminer l'altération des facultés psychophysiques du sujet pour une conduite sûre et, par conséquent, l'élément caractéristique de l'influence. Selon ses propres termes, "les thèses appliquées à l'alcool

¹ Voir : <https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030>.

² Voir : <https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/subsecretaria-del-interior/direccion-general-de-traffic/>

³ Décret législatif royal 6/2015, du 30 octobre, portant approbation du texte révisé de la loi sur le trafic, la circulation des véhicules à moteur et la sécurité routière de l'intérieur. BOE n° 261, du 31 octobre 2015 Référence : BOE-A-2015-11722.

⁴ Positif aux stupéfiants : une amende sera infligée pour infraction à l'art. 14.1. 5^a de la LSV pour présence de stupéfiants (1000 Euros / 6 points)".

⁵ Le conducteur doit utiliser le véhicule avec la diligence, la prudence et le soin nécessaires pour éviter tout dommage à lui-même ou à autrui, en veillant à ne pas se mettre en danger, à mettre en danger les autres occupants du véhicule et les autres usagers de la route, en particulier ceux dont les caractéristiques les rendent plus vulnérables".

ne sont pas transposables en soi aux drogues toxiques, aux stupéfiants et aux substances psychotropes, dont les prémisses scientifiques diffèrent de celles de l'alcool pour diverses raisons", et ce en raison du fait qu'il n'a pas été possible d'établir l'influence sur les aptitudes psychophysiques du sujet lui permettant de conduire en toute sécurité, à partir d'un niveau de concentration de drogue détecté lors d'un test salivaire.

Ainsi, dans notre pays et selon les données fournies par la DGT⁶, "près d'un tiers des personnes tuées dans des accidents de la route dépassaient le taux d'alcoolémie", mais nous pouvons également affirmer, sur la base de l'observation faite pendant plus de deux décennies de pratique professionnelle "sur la route" par l'auteur de ce travail de recherche, que le mode de vie axé sur les loisirs et la vie nocturne est l'un des facteurs qui augmentent la probabilité de consommation d'alcool et de drogues (cannabis, cocaïne et ecstasy) de la part de certains conducteurs (Calafat, A. et al, 2000). Cette consommation s'est consolidée ces dernières années, devenant l'un des principaux facteurs de risque d'accidents de la route en Espagne.

Nous pouvons également affirmer, grâce à l'expérience professionnelle de l'auteur, qu'un autre facteur de risque est le fait d'être passager d'un véhicule à moteur dont le conducteur a consommé de l'alcool ou des drogues, ce qui provoque chaque année un flux constant de ce que nous pouvons appeler des "victimes innocentes" (passagers, motocyclistes, piétons et cyclistes) qui meurent dans des accidents de la route en raison de la conduite d'un conducteur sous l'influence de l'alcool ou de drogues, même après la participation conjointe des deux (conducteur et passager) à des activités nocturnes liées aux loisirs.

C'est pourquoi, malgré les politiques SV de la DGT, les campagnes de sensibilisation à la consommation d'alcool et de drogues avant de prendre le volant et les campagnes de surveillance et de contrôle menées par les agents de la police routière, il n'existe pas encore de véritable "sensibilisation SV communautaire" ou "sensibilisation sociale routière" qui permettrait de comprendre les dangers de ce type de comportement, mais surtout de les prévenir et en tout cas, en tant que conducteur ou usager, de les rejeter et de les dénoncer.

Enfin, nous sommes obligés de mentionner les conducteurs récidivistes ou multirécidivistes (classés comme tels en fonction du temps écoulé entre la commission d'une infraction et une autre et du nombre d'infractions commises) et qui, étant des consommateurs habituels d'alcool ou de drogues (ou des deux substances à la fois), pourraient être appelés "conducteurs dépendants", et qui peuvent être considérés comme potentiellement dangereux pour le SV et devraient donc faire l'objet d'un suivi et d'un traitement spéciaux en tant que patients par les autorités sanitaires⁷, en coordination avec le travail de surveillance et de contrôle effectué par la DGT.

⁶Voir : https://revista.dgt.es/es/noticias/nacional/2022/04ABRIL/0404_Campana-alcohol-Cifal.shtml.

⁷Le règlement national RD 818/2009 Règlement général pour les conducteurs et les règlements européens CD 439/1991, CD 126/2006 et CD 36/2012, stipulent que ces patients (toxicomanes) ne peuvent pas obtenir ou renouveler leur permis de conduire car ils n'ont pas les aptitudes adéquates pour conduire en toute sécurité.

2. LA STRATÉGIE DE LA DIRECTION GÉNÉRALE DE LA CIRCULATION : "TOLÉRANCE ZÉRO".

En juin 2012, la DGT a adopté la mesure de "tolérance zéro" comme principale ligne stratégique en matière de conduite et de consommation de drogues, appliquant cette "tolérance zéro" à tous les conducteurs qui consomment des drogues et qui prennent le volant d'un véhicule. Les raisons invoquées par la DGT⁸ sont les suivantes : "L'Espagne est l'un des pays où la consommation de drogues, en particulier de cocaïne et de cannabis, est la plus élevée, ce qui entraîne un risque accru d'accidents de la route et de blessures graves ou mortelles".

Ainsi, selon l'étude 2017 de l'Observatoire européen des drogues et des toxicomanies (OEDT⁹), dans la tranche d'âge 15-34 ans, l'Espagne est la plus touchée par la toxicomanie dans l'Union européenne :

Le sixième pays de l'UE ayant le taux le plus élevé de consommation de cocaïne (avec une prévalence de 2,8%), après le Royaume-Uni (4,7%), les Pays-Bas (4,5%), le Danemark (3,9%), la France (3,2%) et l'Irlande (2,9%).

Le quatrième pays de l'UE ayant le taux de consommation de cannabis le plus élevé (18,3 %), derrière la France (21,8 %), l'Italie (20,9 %) et la République tchèque (19,3 %).

Par conséquent, les mesures à prendre par la DGT, conformément à sa stratégie de "tolérance zéro", étaient les suivantes :

Sensibiliser l'ensemble de la société au problème, informer les conducteurs du risque lié à la consommation de drogues (sans oublier le risque lié à la consommation d'alcool), connaître la consommation minimale d'alcool et de drogues qui entraîne une altération majeure de la conduite, étendre les contrôles de drogues et d'alcool + drogues sur tous les types de routes, de jours et d'heures, collaborer avec d'autres administrations en matière de législation, d'éducation et de formation liées aux drogues et à la conduite, et promouvoir la recherche appliquée dans le domaine des drogues et de la sécurité routière.

De même, et comme objectif pour l'année 2030, le domaine stratégique de surveillance et de contrôle de la DGT a étendu la "tolérance zéro" aux comportements à risque qui ont le plus d'impact sur les accidents de la route, en fixant comme priorités : l'action sur la vitesse, la consommation d'alcool et de drogues, l'utilisation du téléphone portable au volant et la non-utilisation des équipements de sécurité (ceintures de sécurité, casques, systèmes de retenue pour enfants, etc.)

⁸Document "Drogues et conduite - Tolérance zéro" (DGT).

<https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2012/Presentacion-Tolerancia-cero-con-los-conductores-que-consuman-drogas-al-volante.pdf>

⁹Voir : https://www.euda.europa.eu/publications_en

2.1. RAISON D'ÊTRE ET PROCÉDURE DU DÉPISTAGE SALIVAIRE DES DROGUES.

Jusqu'à une date relativement récente, et en raison de l'absence d'appareils de détection électronique portables (DED) dotés de la technologie appropriée, il n'était pas courant d'effectuer des tests "sur la route" pour détecter si le conducteur avait consommé des drogues. En effet, seule une prise de sang permettait d'être sûr du résultat, mais la réalisation de ces prises de sang et leur transfert au laboratoire pour analyse étaient relativement complexes et difficiles sur le plan juridique.

Par la suite, l'importance de la question et l'engagement de la DGT à détecter la consommation récente de drogues et la présence de drogues dans l'organisme du conducteur sont devenus très pertinents pour le SV et l'environnement de travail du conducteur professionnel. Progressivement, le dépistage des drogues a été mis en place avec des appareils DED portables ⁽¹⁰⁾ qui permettent de détecter et d'analyser la consommation récente de drogues dans la salive du conducteur. Le prélèvement rapide d'échantillons de liquide buccal (procédure non invasive) permet d'obtenir un "résultat positif indicatif" ¹¹ pour l'usage récent de cinq drogues (amphétamines, méthamphétamines, opiacés, cannabis et cocaïne). Toutefois, un deuxième échantillon de salive, appelé "test de preuve", doit être prélevé afin de nommer et de quantifier le type de drogue détecté dans ce deuxième échantillon, et de confirmer ainsi le "positif indicatif" obtenu ; cette deuxième analyse de salive sera effectuée dans un laboratoire de référence. Le transfert au laboratoire de ce "test probant" s'effectue dans un "tube de prélèvement de salive" scellé et identifié par un code-barres, qui est placé dans une glacière, après avoir été enregistré dans un document régi par un protocole strict de chaîne de possession.

Le caractère obligatoire de ce test complémentaire en laboratoire (test probatoire) après le contrôle initial (test circonstanciel) et l'homologation dans le laboratoire de référence du type de drogue détectée et de sa quantité, donnera une présomption de véracité légale à l'infraction pour présence de drogues dans l'organisme du conducteur, ainsi que l'ouverture correspondante d'un dossier de sanction administrative par la DGT.

3. LA DOCTRINE DU BUREAU DU PROCUREUR GÉNÉRAL DE L'ÉTAT À LA SUITE DU TEST SALIVAIRE DE DÉPISTAGE DE DROGUES "POSITIF".

Selon la doctrine du Bureau du Procureur général (FGE)¹², et une fois qu'un "résultat positif" ¹³ a été obtenu dans le test de l'index salivaire effectué dans un DED portable capable d'analyser le fluide oral, l'analyse ultérieure de la salive dans un "laboratoire agréé" est obligatoire, en fonction des activités de contrôle nécessaires de l'administration compétente, garantir également la "chaîne de conservation" ¹⁴ de la salive prélevée pour

¹⁰ Voir : <https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html>

¹¹ Il s'agit d'un échantillon dit "indicatif" qui permet de détecter la **présence** éventuelle de substances illicites. Voir : <https://revista.dgt.es/es/sabia-que/normas/2018/0703como-se-hace-un-control-de-drogas.shtml>

¹² Circulaire 10/2011 du 17 novembre (BOE FIS-C-2001-000010).

¹³ Le terme "positif" n'indique pas un certain taux en nanogrammes, mais tout résultat qui indique la simple présence de drogues dans l'organisme, c'est-à-dire qu'il ne s'agit pas d'un test quantitatif, mais d'un test de qualification avec un résultat positif ou négatif.

¹⁴ La chaîne de contrôle est le processus par lequel il est accrédité que l'objet saisi est le même que celui qui a finalement été analysé. Une éventuelle rupture de la chaîne de contrôle pourrait entraîner une violation du droit à une procédure régulière.

l'analyse afin d'assurer la légalité de la procédure de prélèvement d'échantillons de salive et de leur transformation ultérieure en preuves à charge. Le FGE précise également que les agents chargés de la surveillance du trafic doivent recevoir une formation spécifique pour leur exécution, car ce type de test est plus complexe que les tests de détection d'alcool.

Une fois au laboratoire, les échantillons salivaires sont traités par un équipement analytique composé d'un chromatographe en phase gazeuse¹⁵ (capable de vaporiser des substances de différentes volatilités) et d'un spectromètre de masse¹⁶ (capable de générer des ions à partir de molécules neutres en phase gazeuse, de les séparer en fonction de leur masse et de les détecter en enregistrant l'information de manière appropriée), afin de déterminer le type de drogue et la quantité contenue dans l'échantillon salivaire. Ces kits sont capables de détecter jusqu'à quarante types de drogues et des quantités aussi faibles qu'un nanogramme¹⁷ (ng). Ces résultats de laboratoire sont ensuite examinés un par un par un personnel médical spécialisé, qui signe et valide le rapport final à envoyer à la DGT.

Cependant, comme nous l'avons déjà indiqué, contrairement aux tests d'alcoolémie, une politique de "tolérance zéro" a été adoptée dans le cas des drogues toxiques, puisque le LSV¹⁸ interdit expressément et tacitement la présence de substances narcotiques dans l'organisme du conducteur. Une politique routière qui n'est pas exempte de critiques, puisque plusieurs auteurs reprochent l'écart entre les résultats positifs détectés dans le DED et les résultats positifs en laboratoire (Ramírez, J, 2024).

Ces auteurs précisent qu'il n'est pas possible d'opposer les "cutoff" (seuils analytiques déterminés en ng/ml)¹⁹, des marques de DED portables, les limites de détection confirmées par le laboratoire et la quantité de substance psychoactive détectée.

4. PRÉSENCE DE DROGUES DANS LE CORPS : LA SANCTION ADMINISTRATIVE ET LA DOCTRINE DE LA COUR CONSTITUTIONNELLE.

La LSV impose une sanction administrative de 6 points et une amende de 1000 euros à toute personne qui conduit en présence de stupéfiants dans son organisme. À ce stade, nous mentionnerons la Plénière 174/2017 de la Cour constitutionnelle²⁰ (TC), en raison de la question d'inconstitutionnalité soulevée en relation avec plusieurs articles du RD

¹⁵Voir :

https://www.mncn.csic.es/docs/repositorio/es_ES/investigacion/cromatografia/espectrometria_de_masas.pdf

¹⁶Université de La Rioja. Service de laboratoires et d'ateliers. Chromatographie en phase gazeuse : Analyse qualitative par chromatographie en phase gazeuse avec détection de masse Sans opérations préalables de préparation des échantillons. 75 € / heure. Spectrométrie de masse : Analyse qualitative par spectrométrie de masse électrospray/haute résolution Sans opérations préalables de préparation d'échantillons. 120 € / heure.

¹⁷ Milliardième de gramme : 1 ng = 1e-9 gr.

¹⁸ RD 6/2015 du 30 octobre, modifié par la loi 18/2022 du 20 décembre BOE n° 304. Un seuil est la concentration d'une substance à partir de laquelle un test de diagnostic est considéré comme positif.

¹⁹ Un *seuil* est la concentration d'une substance à partir de laquelle un test de diagnostic est considéré comme positif.

²⁰ BOE n° 15 du 17 janvier 2018. Art. TC.

339/1990²¹, et plus particulièrement sur la pertinence de soulever une question d'inconstitutionnalité en relation avec l'art. 12 de la loi 6/2015, en qualifiant d'infraction administrative la conduite d'un véhicule "avec la présence de drogues dans votre corps", sans qu'il soit nécessaire de prouver que la présence de ces drogues a influencé votre capacité à conduire. La Haute Cour "ne considère pas que les préceptes contestés sont inconstitutionnels parce qu'ils interdisent la consommation de drogues par le biais d'une règle qui vise à protéger la SV". Elle précise également que les préceptes contestés "n'ont pas pour objet d'interdire la consommation de drogues en général". Par conséquent, ce qu'ils interdisent, ce sont les conducteurs qui conduisent "en présence de drogues dans l'organisme (...)". Il s'agit donc d'une "infraction administrative, de sorte que le comportement interdit constituant une infraction administrative n'est pas la consommation de drogues, mais la conduite si ce type de substance a été consommé". Mais ce qui est encore plus intéressant, c'est que la Haute Cour assimile la consommation de drogues toxiques à la consommation de drogues sous prescription médicale et à des fins thérapeutiques, puisque : "Le risque que la conduite avec la présence de ce type de substance dans l'organisme peut entraîner pour la sécurité routière sera le même tant dans le cas où les drogues consommées sont sous indication médicale que dans les cas où la consommation de celles-ci n'est pas à des fins thérapeutiques".

Par conséquent, le TC ne considère pas que les préceptes contestés violent les articles constitutionnels et que cela invalide l'approche et le concept de ce qu'il faut entendre par "drogues" ; en outre, il garantit que ce concept est défini comme une substance qui a une entité suffisante pour altérer les capacités psychophysiques de la personne qui la consomme, et que "L'objectif de la règle, en qualifiant d'infraction administrative la conduite en présence de drogues dans l'organisme, est d'empêcher les personnes de conduire si elles ont consommé des substances susceptibles d'altérer les conditions psychophysiques de la conduite, compte tenu du risque que la conduite dans de telles conditions peut entraîner pour la sécurité du trafic (...)").

5. POINTS DE COUPURE ET QUANTITÉS PSYCHOACTIVES MINIMALES.

Une fois de plus, la DGT avertit, dans le document "Systematic review on drugs in driving" (2021), qu'il n'existe pas d'accords internationaux ou nationaux sur les seuils (quantifiés en ng/ml)²² à établir dans les procédures de contrôle de la consommation de substances chez les conducteurs et que l'Espagne a été l'un des premiers pays à réglementer le dépistage par échantillon de salive. À cette fin, la DGT affirme avoir pris en compte les valeurs recommandées au niveau international dans le domaine de la sécurité au travail, où un certain nombre d'organismes prestigieux, la Substance Abuse and Mental Health Services Administration (SAMHSA)²³ aux États-Unis, la European Workplace Drug Testing Society (EWDTS)²⁴ ... ou le National Safety Council's Alcohol and Drug Testing Society (NSC), ou la National Safety Council's Alcohol, Drugs and Impairment Division (NSC-ADID)²⁵ en Europe et au Royaume-Uni, ont publié des

²¹ BOE n° 63 du 14 mars 1990, approuvant les articles de la loi sur le trafic, la circulation des véhicules à moteur et la sécurité routière.

²² Nanogramme (ng) : unité de masse correspondant à un milliardième de gramme.

²³ Voir : <https://www.samhsa.gov>

²⁴ Voir : <http://www.ewdts.org>

²⁵ Voir : <https://www.nsc.org/workplace/get-involved/divisions/alcohol-drugs-impairment-division>

rapports actualisés sur les recommandations relatives aux seuils à établir, conformément aux exigences des normes ISO²⁶ /IEC²⁷ en Europe.

Ainsi, sur la base de ce qui précède, le ministère de l'intérieur a établi des valeurs de positivité pour l'analyse des preuves en laboratoire, publiées dans le document "Systematic review on drugs in driving" (2021). La DGT prétend ajuster ces valeurs aux recommandations internationales les plus récentes et les plus applicables, ainsi qu'aux preuves générées par l'expérience espagnole dans ce domaine.

TABLEAU 1.

Comparaison des seuils analytiques pour le test de dépistage de la consommation de substances psychoactives dans le liquide buccal chez les conducteurs de la direction générale de la circulation et d'autres organisations internationales.

ANALITO	Seuil salive (ng/ml)			
	EWDTS	SAMSHA	NSC-ADID	DGT
Amphétamine	15	15	15	15
Cocaïne	8	8	8	8
Kétamine	10			10
MDA	15	15	15	15
MDEA	15	15		15
MDMA	15	15	15	15
Méthadone	20		10	10
Méthamphétamine	15	15	15	15
Morphine	15	15	5	5
THC	2	2	2	2

Source : Élaboration propre d'après DGT (2021).
"Revue systématique sur les drogues et la conduite.

Note : EWDTS : European Workplace Drug Testing Society (UK) : EWDTS : European Workplace Drug Testing Society (Royaume-Uni).

SAMHSA : Substance Abuse and Mental Health Service Administration (États-Unis).

NSSC-ADID : National Safety Council - Alcohol, Drugs and Impairment Division (États-Unis).

Analyse comparative des limites de détection (cutoff) des analytes du tableau 1 :

5.1.1 Consensus international : les analytes tels que l'amphétamine, la méthamphétamine, la MDMA, la MDA, la cocaïne et le THC présentent des valeurs homogènes (15 ng/ml pour les stimulants, 8 ng/ml pour la cocaïne et 2 ng/ml pour le THC), ce qui prouve que les normes sont largement acceptées pour leur détection.

5.1.2 Variabilité des analytes spécifiques : la méthadone et la morphine présentent des limites inférieures dans le NSC-ADID et le DGT, ce qui indique des critères plus sensibles, peut-être pour des raisons médico-légales et de sécurité routière.

²⁶ Académie royale d'Espagne : Organisation internationale de normalisation, le système international de normalisation pour la réglementation des produits et des services.

²⁷ Commission électrotechnique internationale, la principale commission de normalisation au monde qui élabore et publie des normes internationales pour les technologies électroniques.

5.1.3. évolution de la norme DGT : la réglementation espagnole de la DGT inclut tous les analytes pertinents, mais adopte également des limites plus strictes dans certains cas, ce qui indique que la priorité est donnée à la détection précoce à des fins de prévention administrative et également pénale.

TABLEAU 2.

Comparaison des seuils (positifs) : DED Sotoxa²⁸, laboratoire SynLab et ceux établis par la DGT.

ANALITO	ABBOT	SYNLAB	DGT
	SOTOXA ²⁹	Laboratoire	DGT ³¹
	TOX400SEU	SYNLAB ³⁰	
6-AM (morphine) (OPI) ³²	40 ng/ml	>2,6 ng/ml	2 ng/ml
Amphétamine (AMP)	50 ng/ml	>18,8 ng/ml	15 ng/ml
Benzoylcgonine (BE)	30 ng/ml	>9,9 ng/ml	8 ng/ml
Métabolite de la cocaïne (COC)	30 ng/ml	>10 ng/ml	8 ng/ml
Codéine (OPI)	40 ng/ml	>12,2 ng/ml	5 ng/ml
Kétamine		>12,6 ng/ml	10 ng/ml
MDA	50 ng/ml	>18,3 ng/ml	15 ng/ml
MDEA	50 ng/ml	>18,2 ng/ml	15 ng/ml
Méthamphétamine (MDMA)	50 ng/ml	>18,7 ng/ml	15 ng/ml
Méthadone (OPI)	40 ng/ml	>12,2 ng/ml	10 ng/ml
Morphine (OPI)	40 ng/ml	>6,2 ng/ml	5 ng/ml
Cannabis (THC)	25 ng/ml	>2,5 ng/ml	2 ng/ml

Source : Élaboration propre (2023) ; sur la base des rapports de la société commerciale SYNLAB, société de surveillance des médicaments et de toxicologie SYNLAB.

Principales observations du tableau 2 :

5.2.1 SOTOXA (DED). Indique les valeurs les plus élevées et reflète des seuils positifs plus permissifs, et non une concentration réelle.

5.2.2. SYNLAB. Signale les valeurs réelles supérieures à un minimum détectable et signale les résultats quantitatifs supérieurs à un seuil, mais n'est pas normatif.

²⁸ Voir : ANNEXE I. Explique la "composition et les principes de fonctionnement de l'analyseur Abbot-SoToxa".

²⁹ Voir : <https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html>

³⁰ Extrait du rapport du test de confirmation des médicaments dans la salive par LC-MS/MS du laboratoire SYNLAB.

³¹ DGT (2021) ; "Systematic review on drug driving" (2021).

³² OPI : Opioïdes.

5.1.3. LA DGT. Fournit les valeurs les plus basses et constitue le seuil légal de confirmation toxicologique, établissant les limites légales de l'infraction administrative et de la sanction correspondante.

6. LA SOCIÉTÉ D'ANALYSE CLINIQUE SYNLAB.

"N'importe quel test, n'importe où, n'importe quand" - telle est la devise de la société allemande Synlab Group (SYNLAB).³³

SYNLAB a été fondé en 1998 par le Dr Bartl Wimmer à Augsburg avec un groupe de partenaires en tant qu'association de médecins de laboratoire indépendants. Depuis lors, l'entreprise s'est développée principalement par le biais d'acquisitions, en proposant des tests de détection du coronavirus pendant la pandémie. SYNLAB n'est pas passé inaperçu auprès des grands investisseurs institutionnels du monde entier qui, au fil des ans, ont pris des participations dans la société. Actuellement, le principal actionnaire est le célèbre fonds de capital-risque britannique Cinven (qui a également un bureau à Madrid), qui détient environ 43 % des actions, selon les estimations de la société allemande. Viennent ensuite les Danois de Novo Holdings (17 %), les Canadiens de l'Ontario Teachers' Pension Fund (OTPP) avec 8 %, soit le même pourcentage que le fondateur de SYNLAB et ses proches associés, et l'État du Qatar par l'intermédiaire de son fonds souverain (5 %).

En Espagne, sa relation avec le ministère de l'Intérieur (selon la plateforme de passation des marchés du secteur public du ministère des Finances) a été forgée par l'intermédiaire de la DGT, qui a lancé un appel d'offres pour le "service de détermination et de quantification des drogues et de l'alcool dans les échantillons de liquide oral et de sang" sur la base d'un contrat³⁴ attribué pour une valeur de 4 999 980,00 euros à SYNLAB DIAGNÓSTICOS GLOBALES S.A.U. (A59845875). Outre la DGT, ce laboratoire clinique a été engagé par d'autres administrations : le gouvernement régional d'Andalousie pour les analyses cliniques du Centre de prévention des risques professionnels de Jaén, le métro de Madrid et la Generalitat de Catalunya³⁵, entre autres.

7. LIMITES DE QUANTIFICATION ET FOURCHETTES D'INCERTITUDE DANS LES RÉSULTATS DES LABORATOIRES SYNLAB.

Le tableau contient des informations supplémentaires sur les échantillons de salive soumis par le laboratoire SYNLAB pour les substances énumérées ci-dessus ; il est utilisé comme "critère de positivité" que la concentration des substances soit supérieure ou égale aux valeurs de la limite de quantification (LOQ)³⁶, plus la "valeur d'incertitude" de l'essai, faute de quoi le résultat est négatif. En outre, SYNLAB fait référence au fait que son laboratoire a "l'incertitude élargie pour K=2 pour l'ensemble de la gamme de travail".

³³ Voir : <https://valenciaplaza.com/asi-es-synlab-empresa-alemana-compra-sistemas-genomicos>

³⁴ Voir : https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfljU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQj_byycwN9yy2dXPLygvNDIoyrVA3Myx1tbfULcnMdAUNYE4U!/ et le BOE 97 du 23 avril 2019.

³⁵ Voir : <https://contractaciopublica.cat/ca/detall-publicacio/200026255>

³⁶ Ce terme désigne la concentration la plus faible qui puisse être obtenue de manière fiable, à condition qu'elle se situe dans les limites de précision spécifiées dans les opérations de routine du laboratoire.

Pour clarifier le concept d'"incertitude", il faut dire qu'il s'agit du "doute" qui peut exister sur le résultat d'une mesure, c'est-à-dire qu'il nous renseigne sur la fiabilité de cette mesure.

Par conséquent, toutes les mesures effectuées présentent une certaine "incertitude" et doivent être quantifiées afin de décider si la mesure effectuée est suffisamment fiable pour l'objectif visé. En outre, il convient de noter que l'"erreur" n'est pas la même chose que l'"incertitude", c'est-à-dire que l'"erreur" n'est pas la même chose que l'"incertitude" :

Erreur : différence entre la valeur mesurée par un appareil et la valeur standard ou de référence³⁷ qui est considérée comme exacte. Lors d'une comparaison entre des valeurs, l'erreur et l'incertitude sont générées conformément à la métrologie. Ainsi, l'erreur et l'incertitude peuvent être utilisées ensemble pour savoir si un instrument se situe dans la limite de l'erreur maximale tolérée.

Incertitude³⁸ : Après avoir effectué plusieurs mesures au cours d'un processus d'étalonnage, on découvre de petites différences entre elles. La moyenne et son écart-type sont déterminés, ce qui permet de déterminer la différence normale entre les mesures et de rendre la mesure finale suffisamment fiable.

Précision : mesure le degré de concordance entre le résultat obtenu et la valeur réelle (ou considérée comme telle).

Précision : indique la concordance entre deux ou plusieurs mesures effectuées de la même manière.

Incertitude élargie³⁹ : Avant de publier la composante d'incertitude combinée, il est nécessaire de multiplier le résultat par la valeur sigma choisie pour obtenir le niveau de confiance requis. Après multiplication, le résultat est l'incertitude élargie, c'est-à-dire l'incertitude avec un niveau de confiance donné.

Évaluation de l'incertitude K=2 : l'étalonnage est effectué par un laboratoire agréé (étalonnage externe) et les données relatives à l'incertitude élargie sont indiquées en %, où K=2 correspond approximativement à un niveau de confiance de 95 %.

Par conséquent, nous pouvons affirmer que les résultats d'analyse des médicaments salivaires du laboratoire SYNLAB ont un niveau de confiance ou une précision attendue qui se situe autour de la fourchette/limite de 95 %.

³⁷ Norme, avec la plus grande précision disponible à un endroit donné ou dans une organisation donnée, et à partir de laquelle les mesures sont dérivées.

³⁸ NSGT (2012) Incertitude d'un résultat de mesure, exprimée sous la forme d'un écart-type expérimental. Ver: <https://www.insst.es/documents/94886/326879/930w.pdf/f657c677-ebab-4f99-8474-667d73e22882>

³⁹ INSGT (2012) : grandeur qui définit un intervalle autour du résultat d'un mesurage et dans lequel on s'attend à trouver une fraction significative de la distribution des valeurs qui pourraient raisonnablement être attribuées au mesurande.

8. LE LABORATOIRE SYNLAB ET SON ACCRÉDITATION PAR L'ORGANISME NATIONAL D'ACCRÉDITATION PAR LE BIAIS D'AUDITS.

L'organisme national d'accréditation (ENAC G-78373214 - C/Serrano 240, 4^a A-B, 28016 Madrid) est le seul organisme désigné par le gouvernement pour opérer en Espagne en tant qu'organisme national d'accréditation⁴⁰, réglementant le fonctionnement de l'accréditation en Europe, qui repose sur cinq principes fondamentaux : "Non lucrativité, indépendance, non-concurrence, évaluation internationale et reconnaissance mutuelle"⁴¹. En outre, l'ENAC peut signer des accords de collaboration avec l'administration générale de l'État et avec les administrations des communautés autonomes, selon ce qui est approprié pour une meilleure exécution de ses activités et de ses fonctions⁴².

L'"accréditation" ENAC devrait être une garantie de l'exécution correcte d'un certain type d'activités, par le biais d'un certificat délivré par cette entité.

À titre d'exemple, l'ENAC a mené les activités suivantes :

En 2013, elle a accrédité l'Instituto de Salud Carlos III⁴³ de Investigación en enfermedades raras selon la norme UNE-En ISO 15189 pour la réalisation des analyses.

Année 2016, "audit externe d'accréditation des activités d'essai et d'inspection technique oculaire" des laboratoires criminels de la Guardia Civil.⁴⁴

Année 2018, a réalisé des "services d'audit" à l'Université de La Corogne.⁴⁵

Année 2022, a accrédité⁴⁶ auprès de la police scientifique de la police nationale pour la "réalisation d'inspections technico-policieres sur les scènes de crime", conformément à la norme ISO 17020.

Pour l'année 2023, il a réalisé des "activités d'accréditation visant à évaluer les laboratoires" de l'Université Complutense de Madrid.⁴⁷

En revanche, en ce qui concerne les activités d'un laboratoire privé (tel que SYNLAB), il peut s'agir d'entités d'essai, d'étalonnage, d'inspection, de certification ou de vérification, entre autres, mais toute activité visant à évaluer si un produit, un service,

⁴⁰ RD 1715/2010 BOE 7 de núm. 7 du 8 janvier 2011, "(...) conformément aux dispositions du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93.

⁴¹ Voir : <https://www.innotec-laboratorios.es/que-es-la-acreditacion-enac/>

⁴² BOE n° 7 du 8 janvier 2011.

⁴³ Voir :

https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IER_sin_anexo_tecnico.pdf

⁴⁴ Voir :

https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IER_sin_anexo_tecnico.pdf

⁴⁵ Voir : https://www.udc.es/export/sites/udc/contratacionadministrativa/contratos-menores/publicar-Dispadic-54.xls_2063069239.xls

⁴⁶ Voir : <https://www.enac.es/actualidad/policia-cientifica-inspeccion-ocular>

⁴⁷ Voir :⁴⁷ <https://www.ucm.es/file/208-2023-enac-1->

un système, une installation, etc. doit être conforme à certaines exigences et peut faire l'objet d'une accréditation.

Ces exigences peuvent être établies par la loi et donc avoir un statut réglementaire, ou être inscrites dans des normes, des spécifications ou d'autres documents volontaires. L'accréditation ENAC permet non seulement à tout laboratoire ou à toute entreprise évaluée de savoir si son activité est exercée correctement, mais elle garantit également l'efficacité maximale de ses services aux clients de ces laboratoires.

Pour évaluer le bon fonctionnement du laboratoire, des audits de suivi annuels sont programmés et, tous les quatre ans, un audit de réévaluation est prévu. Les audits de suivi permettent de vérifier si des modifications ont été apportées aux procédures, si de nouveaux équipements ont été achetés, etc.

En résumé, ce que l'ENAC peut évaluer et certifier, c'est le respect de la norme⁴⁸ UNE-EN ISO/IEC 17025 au cours de l'année en question. Pour information, lors des audits de réévaluation, tous les points de la norme au cours des quatre années précédentes sont passés en revue de manière plus exhaustive. Si le laboratoire ne satisfait pas aux exigences de l'un de ces audits, l'accréditation peut être suspendue.

Pour information, les audits de réévaluation passent en revue de manière plus complète tous les points de la norme au cours des quatre années précédentes. Si le laboratoire ne satisfait pas aux exigences de l'un de ces audits, l'accréditation peut être suspendue.

⁴⁸ BOE 19 du 22 janvier 2018 - Le ministère de l'économie, de l'industrie et de la compétitivité publie les "Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais (ISO/CEI 17025:2017)".

9. TABLEAU 3. PORTÉE DE L'ACCRÉDITATION⁴⁹ ENAC NO. 1169/LE2347, DÉLIVRÉE AUX LABORATOIRES SYNLAB DIAGNÓSTICOS GLOBALES SA., SUR LES ESSAIS (RÉVISÉE LE 23/12/2022).

ORGANISME NATIONAL D'ACCRÉDITATION (ENAC)

PRODUIT/MATIÈRE À TESTER	ESSAI	NORME / PROCÉDURE D'ESSAI																																																																											
<i>PRODUITS/MATIÈRES TESTÉS</i>	<i>TYPE D'ESSAI</i>	<i>SPÉCIFICATIONS STANDARD/PROCÉDURE D'ESSAI</i>																																																																											
Salive (directe ou dans un tampon) Sang total	Détermination quantitative des substances d'abus par chromatographie liquide à haute performance ultra-rapide avec détection par spectrométrie de masse en tandem.	Procédure interne LCMS-004 Rev.15 LCMS-0010 Rev.9																																																																											
Salive (directe ou dans un tampon) Sang	<table> <tr> <th></th><th>LOQ⁵⁰ ng/ml</th><th>LOQ ng/ml</th></tr> <tr> <th>SUBSTANCE</th><th></th><th></th></tr> <tr> <td></td><td>Salive</td><td>Le sang</td></tr> <tr> <td>Morphine</td><td>1</td><td>1</td></tr> <tr> <td>Codéine</td><td>1</td><td>2</td></tr> <tr> <td>Héroïne</td><td>2</td><td>2</td></tr> <tr> <td>Amphétamine</td><td>1</td><td>2</td></tr> <tr> <td>Méthamphétamine</td><td>1</td><td>2</td></tr> <tr> <td>MDA</td><td>2</td><td>2</td></tr> <tr> <td>MDMA</td><td>2</td><td>2</td></tr> <tr> <td>MDEA</td><td>2</td><td>2</td></tr> <tr> <td>Cocaïne</td><td>1</td><td>2</td></tr> <tr> <td>Méthadone</td><td>2</td><td>2</td></tr> <tr> <td>Kétamine</td><td>2</td><td>2</td></tr> <tr> <td>LSD</td><td>2</td><td>2</td></tr> <tr> <td>Clonazepam</td><td>2</td><td>2</td></tr> <tr> <td>Alprazolam</td><td>2</td><td>2</td></tr> <tr> <td>Diazépam</td><td>1</td><td>2</td></tr> <tr> <td>Lorazepam</td><td>2</td><td>2</td></tr> <tr> <td>Oxazepam</td><td>2</td><td>2</td></tr> <tr> <td>Nordiazepam</td><td>1</td><td>2</td></tr> <tr> <td>Tramadol</td><td>1</td><td>2</td></tr> <tr> <td>Phencyclidine</td><td>2</td><td>2</td></tr> <tr> <td>Dextropropoxyphène</td><td>1</td><td>2</td></tr> <tr> <td>Zolpidem</td><td>1</td><td>2</td></tr> </table>		LOQ ⁵⁰ ng/ml	LOQ ng/ml	SUBSTANCE				Salive	Le sang	Morphine	1	1	Codéine	1	2	Héroïne	2	2	Amphétamine	1	2	Méthamphétamine	1	2	MDA	2	2	MDMA	2	2	MDEA	2	2	Cocaïne	1	2	Méthadone	2	2	Kétamine	2	2	LSD	2	2	Clonazepam	2	2	Alprazolam	2	2	Diazépam	1	2	Lorazepam	2	2	Oxazepam	2	2	Nordiazepam	1	2	Tramadol	1	2	Phencyclidine	2	2	Dextropropoxyphène	1	2	Zolpidem	1	2	
	LOQ ⁵⁰ ng/ml	LOQ ng/ml																																																																											
SUBSTANCE																																																																													
	Salive	Le sang																																																																											
Morphine	1	1																																																																											
Codéine	1	2																																																																											
Héroïne	2	2																																																																											
Amphétamine	1	2																																																																											
Méthamphétamine	1	2																																																																											
MDA	2	2																																																																											
MDMA	2	2																																																																											
MDEA	2	2																																																																											
Cocaïne	1	2																																																																											
Méthadone	2	2																																																																											
Kétamine	2	2																																																																											
LSD	2	2																																																																											
Clonazepam	2	2																																																																											
Alprazolam	2	2																																																																											
Diazépam	1	2																																																																											
Lorazepam	2	2																																																																											
Oxazepam	2	2																																																																											
Nordiazepam	1	2																																																																											
Tramadol	1	2																																																																											
Phencyclidine	2	2																																																																											
Dextropropoxyphène	1	2																																																																											
Zolpidem	1	2																																																																											



Source : SYNLAB SYNLAB (élaboration propre)

⁴⁹Voir : https://synlab.es/fileadmin/user_upload/Calidad_docs/Anexo_Tecnico_ISO_17025_version_7.pdf

⁵⁰ LOQ : Limite de quantification ou niveau le plus bas.

OBSERVATIONS CLÉS DU TABLEAU 3 :

9.1. SENSIBILITÉ ACCRUE DE LA SALIVE.

Pour quinze des vingt-deux substances du tableau, la LOQ dans la salive est inférieure à celle dans le sang, ce qui souligne l'efficacité de cette matrice pour la détection précoce de la substance.

9.2. SENSIBILITÉ ÉGALE DES MATRICES POUR CERTAINS COMPOSÉS.

Sept substances (par exemple le LSD, la kétamine, les benzodiazépines) ont la même LOQ dans les deux matrices (2 ng/ml), ce qui indique que la matrice n'affecte pas de manière significative la sensibilité analytique pour ces composés.

9.3. LES IMPLICATIONS CLINIQUES ET MÉDICO-LÉGALES POSSIBLES.

La salive s'est imposée comme une alternative non invasive et très sensible pour l'analyse toxicologique, de sorte que la limite de quantification inférieure de la salive favorise son utilisation dans des contextes tels que les points de contrôle des drogues, les programmes de désintoxication ou la surveillance professionnelle, où l'accès à un test sanguin peut être limité et peu opérationnel.

9.4. ANALYSE SALIVAIRE CONTRE ANALYSE SANGUINE.

La salive s'est positionnée comme une matrice de grande valeur en toxicologie analytique, non seulement parce qu'elle est moins invasive, mais aussi parce qu'elle offre des niveaux de sensibilité plus élevés pour la détection rapide d'une consommation récente.

La détection précoce est particulièrement importante dans les situations de prévention et de contrôle en temps réel, à la fois aux points de contrôle des drogues et dans les accidents de la route impliquant un conducteur sous l'influence possible de ces substances.

L'utilisation de la salive, combinée à une analyse en laboratoire, représente un outil analytique efficace avec une sensibilité supérieure à celle du sang. Ceci en termes de limite de quantification pour un large spectre de substances d'abus.

La recommandation d'intégrer l'analyse salivaire comme matrice de référence dans les protocoles de détection précoce et les diagnostics toxicologiques modernes s'est avérée correcte.

10. CONCLUSIONS.

Premièrement. Les Nations unies invitent les gouvernements et les institutions (publiques et privées), par l'application des lois sur les stupéfiants, à réduire le nombre d'accidents de la route liés à la drogue.

Deuxièmement. En Espagne, la DGT (ministère de l'intérieur) a mis en place une politique de "tolérance zéro" au volant, qualifiant la conduite en présence de drogues dans

l'organisme de comportement à risque. Ce comportement est toujours sanctionné, soit comme une infraction administrative, soit comme une infraction pénale.

Troisièmement. Malgré l'absence d'accords internationaux sur les "seuils", la DGT a établi le "seuil" des quantités psychoactives minimales. Ces quantités sont conformes à celles des organisations publiques et privées de l'UE et des États-Unis. La DGT a ainsi déterminé la positivité quantitative de toute drogue récemment consommée par un conducteur, qui sera ensuite analysée dans le laboratoire de référence.

Quatrièmement. La doctrine du FGE soutient la procédure de collecte d'échantillons salivaires après le test circonstanciel positif, par le biais d'une formation spécifique des agents à la collecte de l'échantillon, de la garantie de la chaîne de conservation et d'une analyse salivaire ultérieure dans un laboratoire de référence.

Cinquièmement. Le TC confirme l'article 14 de la LSV, en précisant que la loi n'interdit pas la consommation de stupéfiants ; ce qu'elle interdit, c'est la conduite avec la présence de stupéfiants dans le corps.

Sixièmement. Le TC met sur le même plan le risque qu'un conducteur ayant consommé des drogues, même sous prescription médicale, peut engendrer pour le SV.

Septièmement. Les "cut-offs" du DED portable (SoToxa Abbott) utilisé pour réaliser le premier "index test", doublent ou triplent les "cut-offs" de référence réalisés par le laboratoire SYNLAB.

Huitièmement. Les "cut-off points" du laboratoire clinique SYNLAB sont plus élevés que ceux déterminés par la norme ISO, que la DGT applique pour établir les quantités psychoactives minimales dans les appareils d'analyse de laboratoire.

Neuvièmement. L'approbation de l'analyse salivaire clinique du laboratoire SYNLAB est avalisée par l'Entité nationale d'accréditation (ENAC), qui certifie la conformité à la norme UNE de l'équipement et de la procédure utilisés par le laboratoire SYNLAB pour obtenir des diagnostics salivaires, tant en ce qui concerne le type de drogue détectée que sa quantité.

Dixièmement. L'évaluation de l'équipement et de la procédure d'obtention de l'analyse des échantillons de salive du laboratoire SYNLAB par l'ENAC, accrédite le niveau de confiance ou de précision de 95% des résultats finaux obtenus et reflétés dans son rapport final.

11. RÉFÉRENCES.

- Abbot. (2020). SoToxa portable toxicology test analyser. https://www.tecmedica.es/cmsAdmin/uploads/o_1f24002cp1ieo17701uni19v4vaja.pdf.
- Abbot. (2020). SoToxa Portable Oral Fluid Analyser (Manuel de l'utilisateur). <https://testdealcoholhydrogas.cl/wp-content/uploads/2022/08/Manual-APOC0798-v2.a-SoToxa-Mobile-Analyser-User-Guide-FWO-LA.pdf>
- Association espagnole de normalisation (2017). Exigences générales concernant la compétence des laboratoires d'étalonnage et d'essais (ISO/IEC 17025:2017). <https://www.une.org/>
- Bequir, S. (2020). Test salivaire de dépistage des drogues, combien de temps dure-t-il ? <https://institutocastelao.com/test-de-droga-en-saliva/>
- Calafat, A et al. (2002). Nightlife recreational life of Spanish young people as a risk factor compared to other more traditional ones. <https://www.redalyc.org/pdf/2891/289122037002.pdf>
- Certum Diagnostics (2019). Test de dépistage des drogues (urine). https://industriasquimicasybiologicas.com/wp-content/uploads/2020/09/Brochure-cassete-individualPrueba-de-Drogas-Certum_Kabla.pdf
- Dirección General de Tráfico (2021). Revue systématique sur les drogues et la conduite. <https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistemica-sobre-drogas-y-conduccion>
- Dirección General de Tráfico (2022). Stratégie de sécurité routière 2030. <https://seguridadvial2030.dgt.es/inicio/>
- Entidad Nacional de Acreditación (n.d.). Brochure institutionnelle de l'ENAC. <https://www.enac.es/actualidad/material-multimedia>
- Organisme national d'accréditation (2022). Rapport 2022. <https://www.enac.es/memoria-2022>
- Ministère public (2021). Circulaire 10/2011 FGE, du 17 novembre, sur les critères de l'unité d'action spécialisée du ministère public en matière de sécurité routière. <https://www.boe.es/buscar/doc.php?id=FIS-C-2011-00010>
- Institut national de toxicologie (2021). Tableau des doses psychoactives minimales des principales substances toxiques faisant l'objet d'un trafic. https://pnsd.sanidad.gob.es/ciudadanos/legislacion/delitos/pdf/20210730_INTF_dosis_minimas_psicoactivas_trafico_de_drogas.pdf
- Observatoire espagnol des drogues et des toxicomanies (2023). Rapport 2023 - Alcool, tabac et drogues illicites en Espagne.

<https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/informesEstadisticas/pdf/2023OEDA-INFORME.pdf>

Observatoire national de la sécurité routière. (2021). Revue systématique sur les drogues au volant. <https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistemica-sobre-drogas-y-conduccion>

Organisation mondiale de la santé. (2021). Plan mondial - Décennie d'action pour la sécurité routière 2021-2030. <https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030>

Ortega Matus, M. (2022). Anticorps monoclonaux et leur utilisation pour identifier la morphine dans les fluides biologiques. <https://riiad.org/index.php/riiad/article/view/riiad-2023-1-09/389>

Parra, M. et Vega, V. (2021). Analyse des drogues d'abus en laboratoire clinique. <https://www.seqc.es/download/tema/38/7601/85888673/142010/cms/tema-9-analisis-de-drogas-de-abuso-en-el-laboratorio-clinico.pdf/>

Ramírez, J. (2024). Los controles de drogas a conductores en España. <https://observatoriocannabis.com/wp-content/uploads/2024/10/controlesdedrogas.pdf>

Ruiz Viera, L. (2018). Anticorps monoclonaux thérapeutiques. <https://riull.ull.es/xmlui/bitstream/handle/915/12352/Anticuerpos+monoclonal+therapeutic.pdf;jsessionid=3462A6DCEAB9DA8E32233B47C6D926E0?sequence=1>

GSC-Laboratoires (2023). Comment évaluer l'incertitude de mesure sans être un expert en mathématiques. <https://sgc-lab.com/guia-para-estimar-la-incertidumbre-de-la-medicion-hecha-para-personas-normales/>

ANNEXE I

COMPOSITION ET PRINCIPES DE L'ANALYSEUR ABBOT-SOTOXA

1.1. COMPOSITION .⁵¹

L'analyseur Abbot SoToxa se compose d'un système d'analyse portable (DED), d'une cartouche ou d'un kit de test et d'un dispositif de collecte de liquide oral.

1.1.1. L'analyseur :

Il s'agit d'un appareil portable de test salivaire numérique, qui utilise des algorithmes pour déterminer l'intensité des lignes de contraste (qui apparaîtront sur la cartouche de test après l'ensemble du processus) et qui peut également afficher sur un écran et imprimer les résultats qualitatifs et nominatifs des drogues détectées.

1.1.2. la cartouche d'essai :

Composé d'une bandelette immunologique⁵² chromatographique⁵³ rapide à usage unique, contenant des réactifs secs et une solution tampon. Ce kit est inséré dans l'analyseur qui le chauffe à la température optimale pour le test.

1.1.3. le dispositif de collecte :

Il s'agit d'un dispositif jetable qui recueille le liquide buccal (salive). Il doit être frotté sur les gencives, la langue et l'intérieur des joues jusqu'à ce que l'indicateur de présence devienne bleu.

1.2. PROCESSUS D'ESSAI :

Le liquide buccal recueilli dans le dispositif de collecte est combiné à la solution tampon, puis mélangé et incubé avant d'entrer en contact avec les bandelettes d'immuno-essai installées dans la cartouche de test à l'aide d'une *"membrane à humidité contrôlée"*.

Le mélange de la solution et de la salive obtenue s'écoule dans le capillaire de la cartouche et entraîne les anticorps anti-médicaments marqués qui y sont déposés. En l'absence de drogue dans l'échantillon, l'anticorps se lie au mélange drogue-protéine en formant une ligne. En présence de drogue, la formation de cette ligne est plus faible.

Le DED lit alors l'intensité des lignes sur la bande d'essai immunologique de la cartouche et compare cette intensité à un seuil prédéterminé de concentration de

⁵¹ Abbott (2020) ; "SoToxa Portable Oral Fluid Analyser" (Manuel de l'utilisateur).

⁵² Un immunodosage chromatographique rapide est utilisé pour la détection quantitative de plusieurs drogues et métabolites de drogues dans la salive, ne fournissant qu'un résultat analytique préliminaire.

⁵³ La chromatographie est une technique utilisée en laboratoire pour séparer les composants de mélanges simples ou complexes. Il existe de nombreux types de chromatographie, de la chromatographie sur papier à la chromatographie sur couche mince en passant par la chromatographie en phase gazeuse.

Voir : <https://www.onelab.com.ar/cromatografia-que-es-y-para-que-sirve-informacion-completa>

médicament, ce qui donne un résultat qualitatif (et non quantitatif). Les résultats sont ensuite affichés sur l'écran du DED et peuvent être imprimés.

1.3. RÉSULTATS POSITIFS.

Le manuel du DED SoToxa d'Abbot précise que les résultats positifs obtenus doivent être confirmés par une seconde méthode telle que la spectrométrie de masse par chromatographie en phase gazeuse (GC-MS). En outre, le DED et ses résultats ne sont pas destinés à un usage domestique, ni à un usage clinique, thérapeutique ou diagnostique.

1.4. COMPOSITION DE LA BANDELETTE D'IMMUNO-ESSAI DE LA CARTOUCHE.

Le dosage immunologique de la chromatocité consiste en une bande imprégnée d'une série de réactifs séchés contenant des anticorps monoclonaux⁵⁴ (mAbs). Ces anticorps (AC) sont des protéines créées en laboratoire et sont utilisés pour identifier les métabolites des drogues d'abus dans les fluides biologiques.

Les AcM ont une sensibilité élevée et se lient, par exemple, à la morphine et à ses métabolites. Ils peuvent donc être utilisés pour produire un résultat marqué en "criblant" la bandelette de test ou la membrane de la cartouche, en détectant de manière sélective des niveaux élevés de drogues spécifiques dans la salive.

⁵⁴ Les anticorps monoclonaux ont aujourd'hui une multitude d'applications, tant dans la recherche biomédicale que dans le diagnostic et le traitement de nombreuses pathologies. Cette qualité des anticorps monoclonaux est due à leur grande spécificité et à leur forte affinité pour la cible thérapeutique.



Article de recherche

PROTECTION DES INFRASTRUCTURES SOUS-MARINES ESSENTIELLES ET RENFORCEMENT DE LA SECURITE DE LA MER BALTIQUE: L'OPERATION BALTIC SENTRY DE L'OTAN

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

Mónica Román González

Candidat au doctorat dans le programme de sciences politiques et
d'administration et de relations internationales à l'université Complutense de
Madrid.

Master en politique internationale : études sectorielles et régionales à l'université
Complutense de Madrid.

monicaromangz@gmail.com

ORCID: <https://orcid.org/0009-0007-8698-3739>

Google Scholar : <https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra>

Reçu le 31/03/2025

Accepté le 28/05/2025

Publié le 27/06/2025

Citation recommandée : Román, M. (2025). La protection des infrastructures sous-marines critiques et le renforcement de la sécurité de la mer Baltique : l'opération Baltic Sentry de l'OTAN. *Revista Logos Guardia Civil*, 3(2), p.p. 221-256.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

PROTECTION DES INFRASTRUCTURES SOUS-MARINES ESSENTIELLES ET RENFORCEMENT DE LA SECURITE DE LA MER BALTIQUE: L'OPERATION BALTIC SENTRY DE L'OTAN

Résumé: INTRODUCTION. 2. CADRE DE L'ÉTUDE. 2.1. L'importance géostratégique de la mer Baltique. 2.2. La protection des infrastructures sous-marines critiques. 2.3. La situation des infrastructures sous-marines critiques dans la mer Baltique depuis le début de l'invasion massive de l'Ukraine par la Russie en 2022. L'OTAN ET LA PROTECTION DES INFRASTRUCTURES SOUS-MARINES CRITIQUES. 4. OPÉRATION BALTIC SENTRY. 5. CONCLUSIONS ET PROPOSITIONS. 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Les dommages causés aux câbles sous-marins dans la mer Baltique ont suscité des inquiétudes quant au potentiel de guerre hybride et à la vulnérabilité des infrastructures sous-marines critiques occidentales face au sabotage, les incidents répétés dans la région étant l'un des principaux exemples des tensions géopolitiques actuelles. L'objectif principal de cet article est d'analyser l'opération *Baltic Sentry* de l'OTAN dans le contexte du besoin croissant de l'Alliance atlantique d'assurer la protection de ce type d'infrastructures critiques dans la zone stratégique de la mer Baltique et de renforcer ainsi la sécurité de cette dernière. Utilisant des méthodes de recherche mixtes, cet article explique tout d'abord l'importance de la protection des infrastructures sous-marines critiques dans la mer Baltique, qui revêt une importance géostratégique, et décrit ensuite le cadre général d'action de l'OTAN pour la protection de ces infrastructures. L'étude présente ensuite les principales caractéristiques de l'opération *Baltic Sentry* lancée par l'OTAN en janvier 2025 et conclut qu'elle répond aux besoins requis pour être une bonne stratégie capable de permettre à l'Alliance de progresser dans la réalisation de deux de ses principaux objectifs prioritaires : la protection d'infrastructures de plus en plus importantes, telles que les infrastructures sous-marines critiques, et le renforcement conséquent de la sécurité dans la mer Baltique afin d'en garantir la résilience.

Resumen: Los daños sobre los cables submarinos en el Mar Báltico han encendido las alarmas sobre una potencial guerra híbrida y la vulnerabilidad de las infraestructuras críticas submarinas occidentales ante posibles sabotajes, siendo así los reiterados incidentes sobre la zona señalada uno de los principales ejemplos de las tensiones geopolíticas existentes en la actualidad. El presente artículo tiene como principal objetivo analizar la Operación *Baltic Sentry* de la OTAN en un contexto en el que impera la creciente necesidad de la Alianza Atlántica de asegurar la protección de este tipo de infraestructuras críticas en el estratégico Mar Báltico y de reforzar así la seguridad sobre este último. Para ello, a través del empleo de métodos mixtos de investigación, el presente artículo primero explica la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico para después exponer el marco general de acción de la OTAN respecto a la protección de estas infraestructuras. Tras ello, el estudio expone las principales características de la Operación *Baltic Sentry* lanzada por la OTAN en enero de 2025 concluyendo que esta se ajusta a las necesidades requeridas para ser una buena estrategia capaz de permitir a la Alianza avanzar en la consecución de dos de sus principales objetivos prioritarios: la protección de unas infraestructuras cuya importancia es cada vez

mayor como son las infraestructuras críticas submarinas y el consiguiente refuerzo de la seguridad en el Mar Báltico en pro de garantizar su resiliencia.

Mots-clés : Organisation du traité de l'Atlantique Nord (OTAN), mer Baltique, infrastructures sous-marines critiques, sécurité, Baltic Sentry.

Palabras clave: Organización del Tratado del Atlántico Norte (OTAN), Mar Báltico, infraestructuras críticas submarinas, seguridad, Baltic Sentry.

ABBREVIATIONS

CCD COE : *Centre d'excellence en coopération pour la cyberdéfense*

CCOE : *Centre d'excellence pour la coopération civilo-militaire*

CMRE : *Centre OTAN de recherche et d'expérimentation maritimes*

CONVEMAR : *Convention des Nations unies sur le droit de la mer*

RRC : *Resilience Reference Curriculum (programme de référence sur la résilience)*

CTF : *Commandant de la force opérationnelle*

GNL : *gaz naturel liquéfié*

GUGI : *Glavnoye upravlenie glubokovodnikh issledovaniï* ou *Direction principale de la recherche en eaux profondes*

MARCOM : *Commandement maritime allié* ou *Commandement naval de l'OTAN (Royaume-Uni)*

OTAN : *Organisation du traité de l'Atlantique Nord*

NSC : *Centre d'expédition de l'OTAN*

OTAN : *Organisation du traité de l'Atlantique Nord*

SOFCOM : *Commandement des forces d'opérations spéciales alliées*

UE : *Union européenne*

URSS : *Union des républiques socialistes soviétiques*

USV : *véhicule de surface sans pilote*

ZEE : *Zone économique exclusive*

1. INTRODUCTION

Ces derniers temps, l'importance des infrastructures sous-marines critiques s'est considérablement accrue, car elles facilitent la fourniture de services de base tels que l'énergie, les transactions financières, les communications ou l'internet. La vulnérabilité de ces infrastructures est donc une préoccupation majeure pour les acteurs internationaux, d'autant plus que le contrôle des fonds marins continue d'apparaître comme un élément déterminant dans les relations de pouvoir de ce siècle (Conte de los Ríos, 2025, p. 34). Si la récente prolifération des technologies sous-marines et l'acquisition conséquente de la capacité à mener des opérations sophistiquées ont favorisé leurs capacités de protection, ces innovations offrent également un éventail de possibilités aux acteurs qui souhaitent exploiter leurs faiblesses (Cassetta, 2024, p. 2).

En ce sens, toute attaque contre l'infrastructure sous-marine de l'Organisation de l'Atlantique Nord (OTAN) aurait de graves conséquences pour la sécurité de ses Etats membres, faisant d'elle une cible pour ses rivaux. Sachant qu'une attaque contre ces câbles nécessite la disponibilité de moyens précis, la Russie et, dans une moindre mesure, la Chine sont les pays qui pourraient être identifiés comme la menace la plus directe, selon l'Insikt Group (2023, p. 11-15) dans son dernier rapport sur les risques pour les câbles sous-marins.

Ainsi, la "*guerre des fonds marins*", plus communément appelée *Seabed Warfare*, constitue désormais une menace immédiate pour l'Alliance atlantique. Des épisodes tels que les incidents répétés impliquant des câbles sous-marins dans la région géostratégique de la mer Baltique soulignent l'ampleur des risques posés par une menace qui nécessite des efforts et des investissements coordonnés pour compléter les stratégies conçues par chaque Etat. C'est là que la nouvelle opération de l'OTAN visant à protéger les infrastructures sous-marines essentielles en mer Baltique - l'opération *Baltic Sentry* - entre en jeu.

Il existe un large éventail de publications sur cette question. D'une part, les principales raisons qui expliquent l'importance de la protection des infrastructures sous-marines critiques sont largement couvertes par les recherches d'experts en la matière tels que Noelia Arjona Hernández (2023), Rafael García Pérez (2024) et Augusto Conte de los Ríos (2025). En revanche, en ce qui concerne le rôle de l'OTAN dans la protection de ces infrastructures, le rapport de Njall Trausti Fridbertsson (2023) ou l'article de Sean Monaghan, Otto Svendsen, Michael Darrah et Ed Arnold pour le *Center for Strategic & International Studies* (2023) sont dignes d'intérêt. À la lumière de ces éléments, l'objectif global de cette étude est d'analyser l'opération *Baltic Sentry* récemment annoncée dans le cadre de l'OTAN visant à renforcer la sécurité de la mer Baltique par la protection des infrastructures sous-marines essentielles.

En conséquence, la question de recherche globale qui guide cette étude est la suivante : comment l'opération *Baltic Sentry* de l'OTAN répond-elle à la protection des infrastructures sous-marines essentielles en mer Baltique ? L'hypothèse générale de la recherche est que l'opération *Baltic Sentry* renforce la protection des infrastructures sous-marines essentielles en mer Baltique et la présence de l'Alliance en mer Baltique, s'adaptant ainsi au nouvel environnement de menace.

À cette fin, deux objectifs spécifiques ont été définis. Premièrement, expliquer l'importance de la protection des infrastructures sous-marines critiques dans une zone de grande importance géostratégique comme la mer Baltique, en particulier dans le contexte international actuel marqué par la menace russe suite à son invasion de l'Ukraine et

l'augmentation des dommages subis par ce type d'infrastructures depuis lors. Deuxièmement, définir le cadre général d'action de l'OTAN en matière de protection des infrastructures sous-marines critiques.

Ainsi, après avoir utilisé des méthodes de recherche mixtes, l'étude se termine par des conclusions concernant le nouveau projet de l'OTAN, qui tente de répondre à deux questions de sécurité de plus en plus importantes : la protection des infrastructures sous-marines essentielles et le renforcement de la sécurité de la mer Baltique qui en découle.

2. CADRE DE L'ÉTUDE

2.1. L'IMPORTANCE GÉOSTRATÉGIQUE DE LA MER BALTIQUE

Située au nord de l'Europe (voir figure 1), la mer Baltique est historiquement une zone de compétition géopolitique, qui est aujourd'hui réapparue comme un point crucial de menace pour la sécurité européenne suite à l'invasion de l'Ukraine. Au-delà de ses avantages commerciaux et de ses ressources marines, cette enclave est une plaque tournante essentielle pour les infrastructures qui contribuent de manière significative à l'approvisionnement énergétique de plusieurs États européens, eux-mêmes membres de l'OTAN (Fridbertsson, 2023, p. 2).

L'Alliance elle-même le définit comme "une plaque tournante vitale pour le commerce et le transport d'énergie reliant de nombreux pays alliés" en étant un conduit pour les approvisionnements en énergie et un support pour les câbles sous-marins qui transfèrent des données, deux éléments cruciaux pour l'économie et la sécurité des Alliés (Commandement maritime allié de l'OTAN, 2025a).

Figure 1

Carte politique de la mer Baltique.



Source : McNamara (2016) : McNamara (2016).

Avec l'adhésion de la Finlande et de la Suède à l'OTAN en 2023 et 2024, la mer Baltique est devenue le "lac de l'OTAN". Cette appellation n'est toutefois pas suffisante si l'on considère que les alliés de la région sont toujours confrontés à de nombreuses menaces et, comme le définit John Deni (2023), à un paysage sécuritaire régional dynamique qui les oblige à unir leurs forces par le biais des différents cadres de coopération à leur disposition. Cette situation découle principalement de la présence de la Russie dans la région, qui pose des défis croissants à la sécurité des alliés, en particulier dans le contexte qui fait de la protection du flanc dit oriental de l'OTAN une question de sécurité prioritaire.

Historiquement, la Russie est un acteur majeur dans la région de la Baltique. D'une part, elle dispose de la ville portuaire de Saint-Pétersbourg, centre économique et culturel important du pays, par lequel transite la majeure partie de son commerce maritime depuis l'époque de Pierre le Grand. D'autre part, la Russie contrôle également l'enclave de Kaliningrad entre la Pologne et la Lituanie, où elle dispose de bases militaires avec la flotte de la Baltique (Savitz et Winston, 2024, p. 5).

En outre, la "flotte fantôme russe", une flotte de pétroliers créée par le Kremlin qui navigue sous le pavillon d'autres pays afin d'échapper aux sanctions imposées après son agression illégale contre l'Ukraine, opère actuellement dans la mer Baltique (Childs, 2025, p. 5). Comme d'autres navires russes, celui-ci est équipé d'une technologie capable de surveiller les fonds marins et est donc également soupçonné de participer à la campagne hybride de la Russie contre l'Occident par la collecte de renseignements et la préparation ultérieure du sabotage d'infrastructures sous-marines critiques (Jones, 2025, p. 8). À cela s'ajoute le fait que Moscou a démontré à plusieurs reprises ses ambitions expansionnistes dans une région qui pourrait être sa prochaine cible, en particulier au plus fort de son hostilité envers l'OTAN.

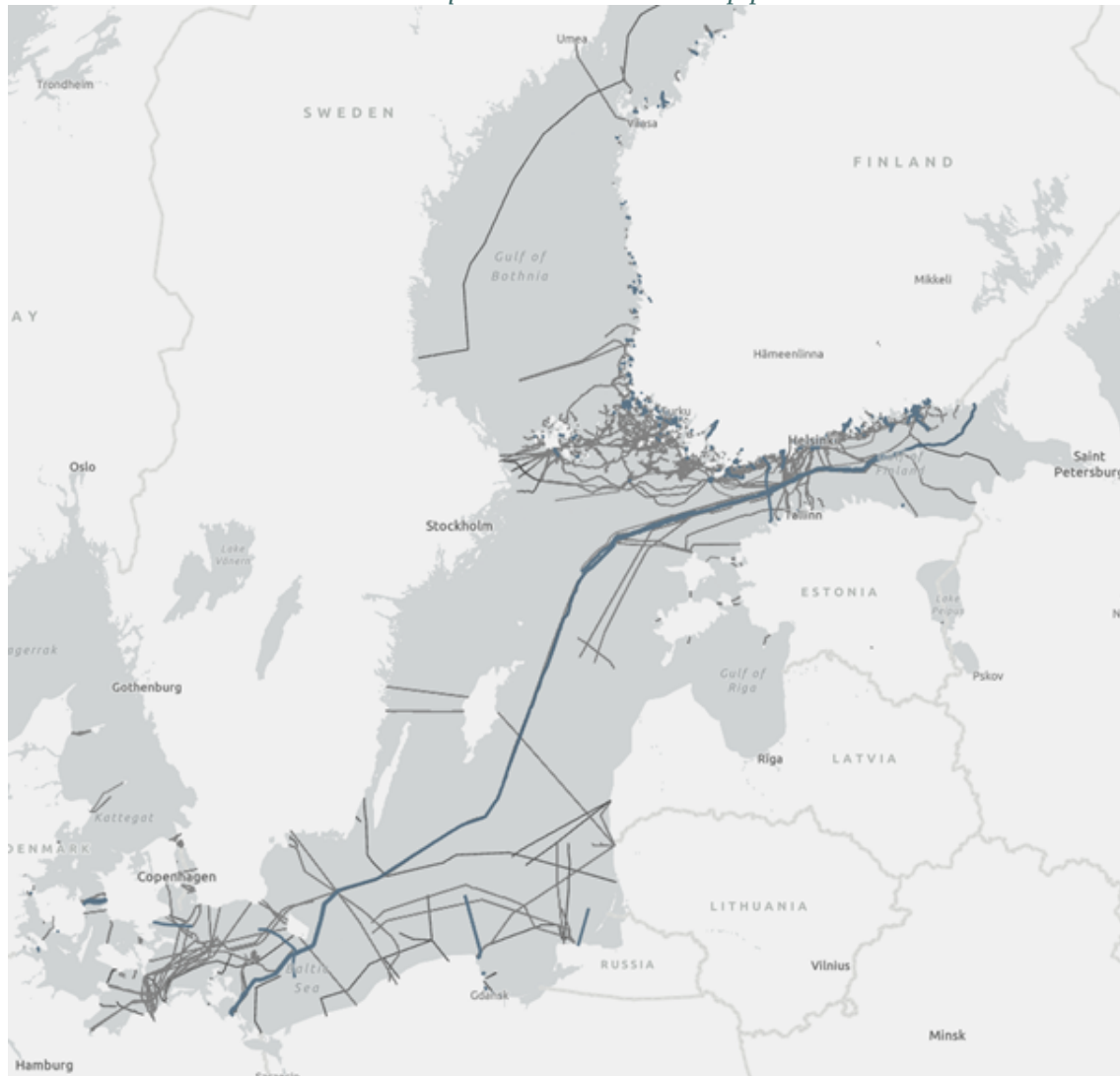
Par conséquent, la Russie constitue le principal défi pour l'Alliance dans la région. Dans la région, Moscou considère les tactiques hybrides comme le principal outil pour faire pression sur les alliés afin d'atténuer les faiblesses militaires conventionnelles et de minimiser les risques de provoquer une confrontation directe entre les parties (Cassetta, 2024, p. 2). Comme on le sait, les sabotages sont exécutés d'une manière qui rend difficile l'identification des responsables, ce qui incite les pays concernés à faire preuve de prudence dans l'attribution des responsabilités par crainte d'une escalade. Ils sont donc utiles à la Russie pour miner l'OTAN en empêchant l'activation de l'article 5 de la défense collective (Jones, 2025, p. 3).

Dans le même temps, il convient de noter que les capacités sous-marines de la Russie constituent son principal atout pour affronter la concurrence dans la région. Comme l'explique Sidharth Kaushal (2023), Moscou dispose de la Direction principale de la recherche en eaux profondes (*Glavnoye upravlenie glubokovodnikh issledovaniï*, GUGI), une agence secrète dépendant du ministère russe de la défense qui exploite des sous-marins et des navires capables de se livrer à des actes de sabotage.

Étant donné que les capacités d'attaque des infrastructures critiques de la Russie constituent un élément fondamental de sa stratégie (Fink et Kofman, 2020, p. 16), elles pourraient être utilisées pour intercepter des communications critiques dans la région de la Baltique (Metrick et Hicks, 2018, p. 7). Cette région abrite un réseau complexe

d'infrastructures sous-marines qui sont essentielles à la communication et à l'approvisionnement en énergie entre les nations européennes (voir figure 2).

Figure 2
La mer Baltique : carte des câbles et pipelines.



Source : Commission de protection de l'environnement marin de la Baltique (2024).

La protection de ces infrastructures maritimes critiques dans cette région géostratégique clé dépend fortement de l'OTAN (Fridbertsson, 2023, p. 11), ce qui ouvre une fenêtre d'opportunité pour Moscou dans sa volonté d'affaiblir l'Occident.

2.2. PROTECTION DES INFRASTRUCTURES CRITIQUES SOUS L'EAU

Les communications, les transactions financières, l'énergie et un large éventail d'activités quotidiennes essentielles dépendent d'infrastructures sous-marines critiques. Selon les données fournies par le *Submarine Telecoms Forum* (2025, p. 8-9) dans son dernier rapport, 99 % du trafic international de données transite par les câbles sous-marins, ce qui en fait "l'épine dorsale des communications mondiales".

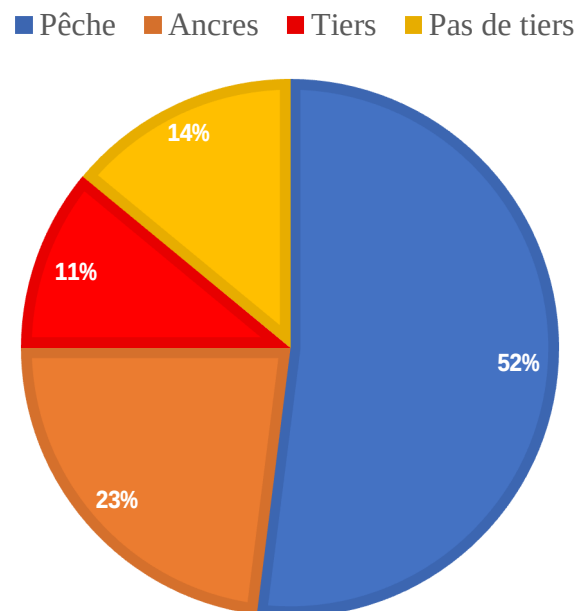
Son importance est telle que toute atteinte peut avoir de graves conséquences sur la stabilité de la société, ce qui confère à sa sécurité une importance géostratégique

capitale et en fait un bien inestimable dont la protection doit être une priorité dans les agendas de sécurité (Quijarro Santibáñez, 2023, p. 15-22) (Fridbertsson, 2023, p. 2) (García Pérez, 2024, p. 265-298).

La dépendance croissante à l'égard des infrastructures critiques sous-marines et la convergence actuelle des menaces traditionnelles et émergentes font de leur protection l'un des plus grands défis en matière de sécurité (Conte de los Ríos, 2025, p. 26), compte tenu notamment de leur vulnérabilité aux menaces naturelles et anthropiques (Guilfoyle, Paige et McLaughlin, 2022, p. 657-696). Le *Comité international de protection des câbles* (2024, p. 5) affirme que l'interaction humaine est la cause la plus fréquente de dommages aux câbles, généralement causés par la pêche et les ancres (voir figure 3).

Figure 3

Tableau des principales causes de rupture des câbles selon le Comité international de protection des câbles.



Source : Comité international de protection des câbles (2024, p. 5) Comité international de protection des câbles (2024, p. 5).

Dès 2016, face à l'augmentation de l'activité sous-marine russe dans des proportions jamais connues depuis la guerre froide, James Foggo et Alarik Fritz (2016) ont proposé leur idée de l'existence de "La quatrième bataille de l'Atlantique" dans laquelle les infrastructures sous-marines, notamment les plateformes d'approvisionnement en énergie et les câbles de télécommunication, seraient menacées. Une bataille qui, selon James Foggo (2023), a véritablement commencé après l'attaque apparente du gazoduc Nord Stream en 2022.

Le fait est que l'importance de ces infrastructures en a fait non seulement une cible prioritaire pour la protection, mais aussi une cible possible pour les attaques d'acteurs intéressés par la déstabilisation. Des incidents tels que celui mentionné ci-dessus ont fait prendre conscience de la vulnérabilité de ces infrastructures dans le contexte des tensions internationales, ce qui a constitué un tournant dans la compréhension du fait que

l'adoption de mesures visant à garantir leur protection est fondamentale (Fridbertsson, 2023, p. 11) (Monaghan et al., 2023, p. 2).

D'autre part, l'évolution technologique constante a d'importantes répercussions sur les capacités sous-marines que les différents acteurs doivent acquérir (Clark, 2015, p. 18), ce qui a contribué de manière significative à la consolidation du domaine sous-marin en tant que "sixième domaine". Ce nouveau domaine opérationnel, de plus en plus contesté, concentre des intérêts économiques, stratégiques et militaires en raison de la richesse des ressources qu'il recèle et qui en font un théâtre de conflit connu sous le nom de *guerre des fonds marins* (Conte de los Ríos, 2025, pp. 29-30). Bien que sa conceptualisation soit encore en cours d'élaboration par des acteurs tels que l'OTAN, Conte de los Ríos (2025, p. 29) la définit comme l'ensemble des opérations menées dans, vers, depuis, sur et sous les fonds marins à des fins stratégiques ou militaires, en utilisant le sabotage du gazoduc Nord Stream comme cas représentatif.

Le domaine maritime est particulièrement vulnérable aux menaces hybrides. Outre le fait que ces dernières sont difficiles à distinguer des dommages accidentels, les agresseurs peuvent utiliser la couverture de navires de diverses natures difficiles à suivre, tels que des bateaux de pêche ou des navires privés (Monaghan et al., 2023, p. 6). À cet égard, il convient de rappeler que, le sabotage n'étant pas considéré comme une violation de l'interdiction du recours à la force en vertu de la Charte des Nations unies, le droit international limite la réponse militaire aux dommages causés aux câbles, en particulier lorsque des navires non militaires sont impliqués (Conte de los Ríos, 2023, p. 33).

Christian Bueger et Tobias Liebetrau (2021) affirment que la gouvernance des infrastructures critiques sous-marines est plus complexe en raison de deux facteurs : (1) la nécessité d'une coopération internationale entre divers acteurs étatiques - qui agissent sur la base de leurs avantages stratégiques - et (2) le fait qu'une partie de ces infrastructures appartiennent au secteur privé - dont le rôle est pertinent compte tenu du fait que leurs intérêts peuvent ne pas être alignés sur ceux des États -. Cette complexité rend difficile l'application de dispositions juridiques efficaces en cas de dommages causés aux infrastructures sous-marines critiques (Conte de los Ríos, 2023, p. 32).

Le régime juridique applicable aux infrastructures sous-marines s'appuie sur des instruments internationaux, parmi lesquels se distinguent la Convention pour la protection des câbles télégraphiques sous-marins de 1884 et la Convention des Nations unies sur le droit de la mer (CNUDM) de 1982. Cette dernière établit que tous les États ont le droit d'installer des câbles sous-marins et des pipelines sur le plateau continental, conformément à la législation nationale de l'État côtier concerné (Arjona Hernández, 2023, p. 48). De même, la CNUDM délimite différents espaces maritimes - les eaux territoriales, les zones économiques exclusives (ZEE) et la haute mer - en attribuant une souveraineté totale dans les premières, des droits limités dans les ZEE et un cadre réglementaire moins bien défini dans les eaux internationales, où l'activité militaire d'autres États ne peut être légalement restreinte (McNamara, 2024).

Il convient de noter que parmi les défis émergents pour le droit maritime international figurent les véhicules sous-marins sans pilote (UUV) et les systèmes maritimes sans pilote (MUS), dont le statut juridique reste indéfini. L'absence d'un cadre réglementaire spécifique pour leur exploitation internationale complique leur intégration dans les régimes actuels, notamment en ce qui concerne la CNUDM (Conte de los Ríos, 2023, p. 32). Dans ce contexte, l'importance croissante des infrastructures sous-marines critiques rend essentielle la progression vers un cadre juridique international efficace qui garantisse leur protection (García Pérez, 2023, p. 50).

Compte tenu de l'importance de ces infrastructures et de leur législation complexe, Michael McNamara (2024) explique qu'à mesure que les tensions géopolitiques entre l'Occident et ses concurrents augmentent, ces infrastructures sont une cible car l'ingérence hybride est un outil utile dans son objectif de remettre en cause les intérêts des démocraties euro-atlantiques. Celles-ci sont actuellement menacées par les actions hybrides de la Russie (Monaghan et al., 2023, p. 2), en particulier dans la mer Baltique où elle a renforcé sa présence en investissant dans des capacités sous-marines, considérées comme son principal atout (Gresh, 2023, p. 3-4).

Compte tenu du contexte complexe et de la situation de la mer Baltique, des experts tels que Conte de los Ríos (2025), Njall Trausti Fridbertsson (2023) et Monaghan et al (2023) s'accordent sur une série d'éléments clés pour définir une stratégie de protection efficace. Reconnaissant qu'il est essentiel de renforcer les capacités de détection, de dissuasion-prévention, d'adaptation et de réponse, les éléments à mettre en avant sont : (1) une présence ou une surveillance accrue, (2) une collaboration entre les acteurs, (3) une coordination avec le secteur privé, (4) une technologie avancée, (5) des cadres réglementaires, (6) des mesures de réponse et (7) le renouvellement des stratégies maritimes.

2.3. LA SITUATION DES INFRASTRUCTURES SOUS-MARINES CRITIQUES DANS LA MER BALTIQUE DEPUIS LE DÉBUT DE L'INVASION RUSSE DE L'UKRAINE EN 2022

Le 26 septembre 2022, l'autorité maritime danoise a signalé plusieurs fuites de méthane causées par une série d'explosions sous-marines au large de l'île danoise de Bornholm, qui ont gravement endommagé le gazoduc Nord Stream (voir figure 4), interrompant l'approvisionnement en gaz russe du marché européen via le gazoduc Nord Stream (Energistyrelsen, 2022).

Figure 4

Carte des gazoducs Nord Stream 1 et Nord Stream 2 à proximité des fuites de méthane détectées en septembre 2022.



Source : Agence spatiale européenne (2022) Agence spatiale européenne (2022).

Indépendamment de l'auteur inconnu de ce sabotage apparent, les experts s'accordent à dire qu'il s'agit là d'un tournant qui a incité les Alliés à envisager des efforts pour améliorer leur capacité à se défendre contre les tactiques hybrides dans le domaine sous-marin (Monaghan, 2022) (Fridbertsson, 2023) (Conte de los Ríos, 2025).

Un cas similaire a été enregistré en octobre 2023 avec l'incident du gazoduc Balticconnector. Cette infrastructure, ainsi que le terminal de gaz naturel liquéfié (GNL) d'Inkoo, garantit la sécurité d'approvisionnement et l'indépendance énergétique des pays de la région (voir figure 5).

Figure 5
Carte du réseau de transport de gaz en Finlande et dans les États baltes.



Source : Gasgrid (n.d.)

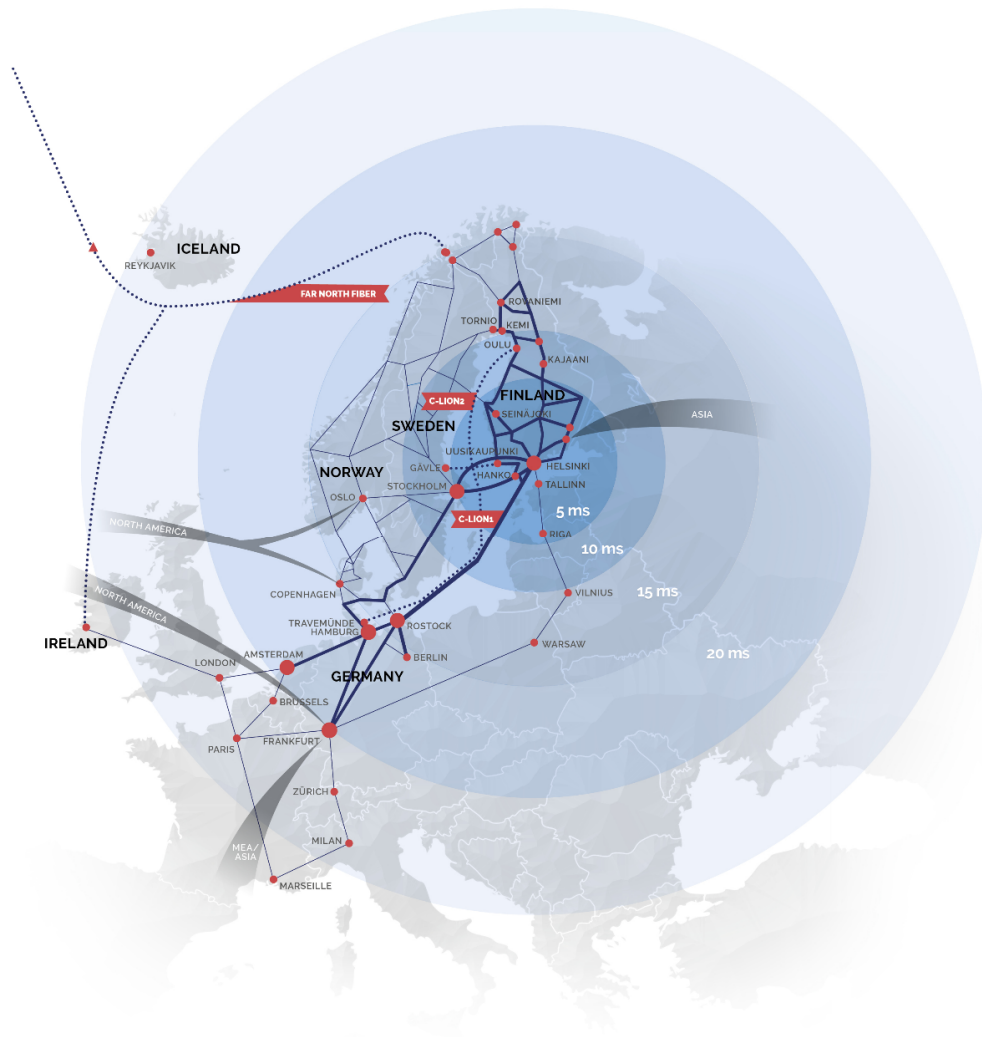
Selon les données fournies par le Bureau national d'enquête finlandais, les dommages causés à l'oléoduc ont probablement été provoqués par le Newnew Polar Bear de la compagnie maritime chinoise, qui a poursuivi son voyage vers les eaux russes, escorté par un brise-glace de l'État eurasiatique (Police of Finland, 2023a). En outre, le Sevmorput, un cargo russe à propulsion nucléaire, a également été détecté dans la zone au cours de l'incident (Police of Finland, 2023b).

L'implication présumée de la Russie dans cette attaque pourrait viser à déstabiliser l'approvisionnement énergétique de ces pays, qui dépendaient fortement du gaz russe jusqu'à ce qu'il soit interdit en réponse à l'invasion de l'Ukraine (Lietuvos Respublikos Energetikos Ministerija, 2022) (Latvijas Vēstnesis, 2022) (République d'Estonie Ministère des affaires étrangères, 2022) (Ministère des affaires économiques et de l'emploi de la Finlande, 2024). En 2014 déjà, alors que les États baltes tentaient d'accélérer leur déconnexion de l'approvisionnement russe par la synchronisation de leurs réseaux électriques avec le soutien de l'Union européenne (UE), la Lituanie a signalé des cas d'interférence par des navires militaires russes dans l'installation de NordBalt, un câble électrique sous-marin reliant le pays à la Suède (McNamara, 2024).

En novembre 2024, le câble sous-marin C-Lion1, appartenant à la société finlandaise Cinia, a apparemment été délibérément endommagé. Ce câble étant essentiel à la communication directe entre la Finlande et l'Allemagne (voir figure 6), l'avarie a entraîné l'interruption des télécommunications entre les deux États. La gravité de l'affaire était telle que les ministres des affaires étrangères de ces pays ont déclaré dans une déclaration commune que les soupçons d'une attaque intentionnelle étaient élevés, notant que "la sécurité européenne n'est pas seulement menacée par la guerre d'agression de la Russie contre l'Ukraine, mais aussi par la guerre hybride d'acteurs malveillants" et demandant instamment le renforcement de la défense de ce type d'infrastructure dans la région (ministère des affaires étrangères de la Finlande, 2024).

Figure 6

Carte de la connectivité entre les États nordiques et l'Europe centrale via les câbles sous-marins C-Lion1 et C-Lion2.



Source : Cinia (n.d.) : Cinia (n.d.)

Simultanément, le câble de télécommunications BCS East-West Interlink reliant la Lituanie et la Suède a été endommagé à la suite de "plus qu'un simple accident", comme l'a déclaré Andrius Šemeškevičius, directeur de la technologie de la société Telia Lietuva, au radiodiffuseur national lituanien LRT TV (2024).

Les enquêtes menées par les pays concernés par les deux incidents se sont concentrées sur le navire chinois Yi Peng 3, qui avait auparavant quitté le port russe d'Ust-Luga. Ne pouvant monter à bord du navire, les forces navales danoises ont surveillé de près sa situation une fois qu'il est entré dans le détroit de Kattegat, comme cela a été confirmé sur leurs médias sociaux (Forsvaret, 2024). D'après les déclarations de Šemeškevičius à LRT TV (2024), la probabilité d'un sabotage est assez élevée, car les câbles des deux incidents se croisent (voir figure 7).

Figure 7

Carte des câbles sous-marins endommagés en mer Baltique en novembre 2024 et localisation du navire Yi Peng 3.

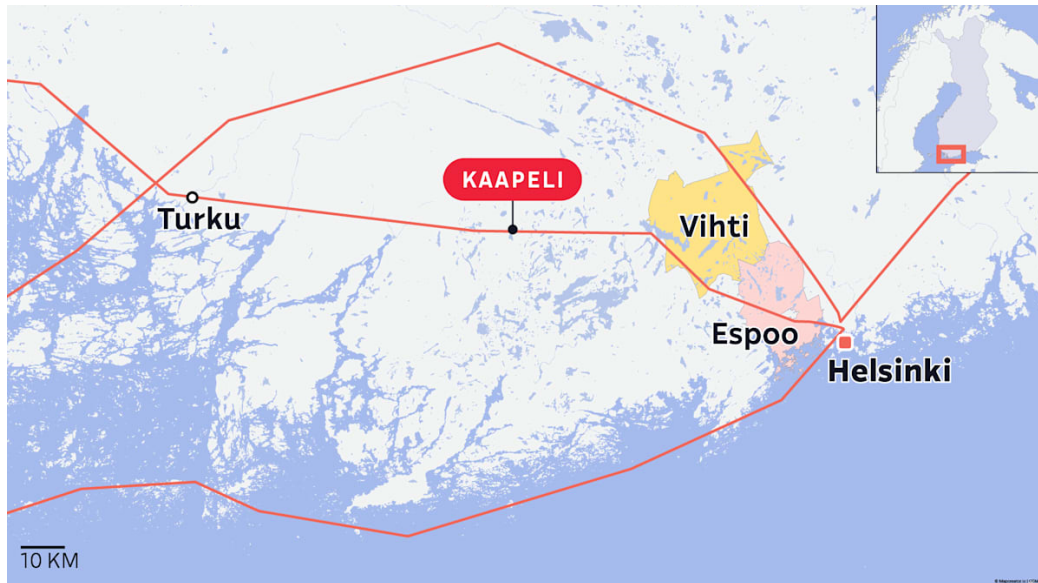


Source : Reuters (2024) Reuters (2024).

Un mois plus tard, le 3 décembre 2024, la société finlandaise GlobalConnect a signalé que ses câbles de télécommunications reliant le pays à la Suède avaient été endommagés en deux points distincts entre les régions de Vithi et d'Espoo (voir figure 8), comme l'a confirmé le responsable de la communication de la société, Niklas Ekström, au radiodiffuseur public finlandais Yle (2024a). Cependant, la police finlandaise a déclaré dans un communiqué qu'il n'y avait aucune indication de sabotage, mais plutôt d'un accident dû à des dommages causés lors des excavations (Police of Finland, 2025a).

Figure 8

Carte du câble sous-marin de la société finlandaise GlobalConnect endommagé en décembre 2024.



Source : Yle (2024b) : Yle (2024b).

Le 25 décembre 2024, l'opérateur finlandais Fingrid signale que le câble sous-marin Estlink 2 du réseau électrique reliant la Finlande et l'Estonie a été endommagé (voir figure 9). La Finlande ouvre une enquête pour sabotage et saisit le pétrolier russe "Ghost Fleet" Eagle S, qui transportait du pétrole russe dans la zone et qui a apparemment causé les dommages en tirant son ancre (Police of Finland, 2025b). Cet événement a incité l'OTAN à annoncer, fin décembre, son intention de renforcer sa présence militaire en mer Baltique afin de prévenir de nouveaux incidents et de faire face à d'éventuelles nouvelles menaces pesant sur ces infrastructures (OTAN, 2024a).

Figure 9

Carte de la connectivité entre la Finlande et l'Estonie via les câbles sous-marins Estlink 1 et Estlink 2.

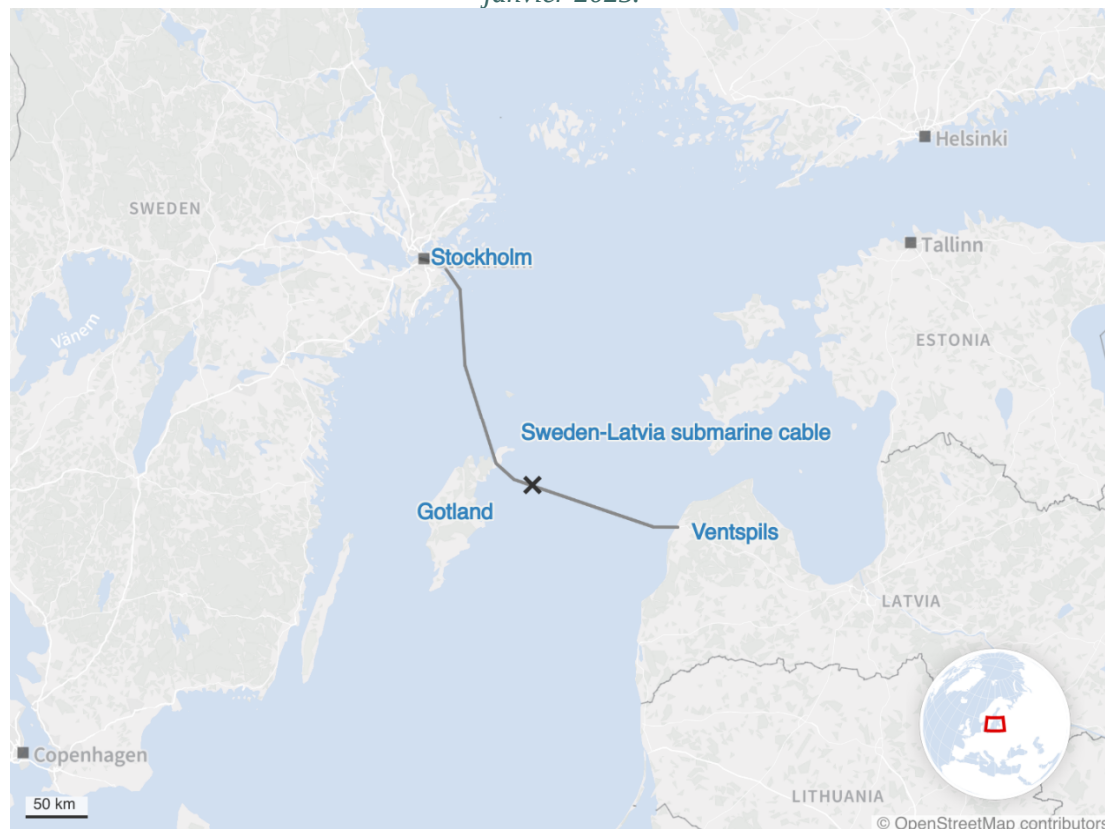


Source : Fingrid (n.d.) : Fingrid (n.d.).

Le 26 janvier 2025, un câble de communication entre la Suède et la Lettonie a été endommagé (voir figure 10), comme l'a indiqué la société responsable, le Latvia State Radio and Television Center (2025). Bien que le pays nordique ait ouvert une enquête préliminaire pour sabotage et saisi le cargo bulgare Vezhen, le parquet suédois a finalement déterminé que la rupture du câble entre les deux pays n'était pas le résultat d'une attaque délibérée mais d'un accident (Swedish Prosecution Authority, 2025). De même, à la demande des autorités lettones, la Norvège a saisi le Silver Dania, avec équipage russe, qui naviguait entre Saint-Pétersbourg et Mourmansk (Politiet, 2025).

Figure 10

Carte du câble sous-marin de la mer Baltique reliant la Lettonie et la Suède endommagé en janvier 2025.



Source : Reuters (2025) : Reuters (2025).

En février 2025, un autre câble sous-marin reliant la Finlande et l'Allemagne a été endommagé dans la ZEE suédoise, près de l'île suédoise de Gotland. Alors que la Finlande a déjà lancé une enquête sur l'endommagement du câble appartenant à l'une de ses entreprises (Police de Finlande, 2025c), la Suède évoque la possibilité d'un sabotage. Patrik Johansson, chef du département de l'eau et de l'assainissement dans la région touchée de Gotland, a confirmé après le premier examen du site que la cause principale était l'influence humaine (Region Gotland, 2025).

Simultanément, la société finlandaise Cinia (2025) a de nouveau signalé des perturbations dans le fonctionnement du câble sous-marin C-Lion1. Bien que l'enquête soit toujours en cours, le média allemand Kieler Nachrichten (2025) a rapporté que les autorités allemandes ont enquêté sur le cargo Arne, un navire soupçonné de faire partie de la "flotte fantôme russe", qui naviguait dans la région sous le pavillon d'Antigua-et-

Barbuda et se dirigeait de Saint-Pétersbourg à Séville sans l'une de ses ancrs, ce qui a fait naître des soupçons de sabotage apparemment orchestré par le Kremlin.

Ces incidents démontrent que les infrastructures sous-marines critiques de la région sont vulnérables aux attaques. En 2017 déjà, le commandant de la force sous-marine de l'OTAN, Andrew Lennon, a confirmé l'existence d'une "activité sous-marine russe à proximité des câbles sous-marins" à des niveaux jusqu'alors inconnus, soulignant l'intérêt stratégique de la Russie pour l'infrastructure sous-marine de l'OTAN (Birnbaum, 2017). Comme le notent Monaghan et al. (2023, p. 1), ces attaques potentielles "visent à perturber la cohésion transatlantique et l'activité économique, à saper le soutien de l'Occident à l'Ukraine et à façonner d'éventuelles futures opérations militaires". La situation depuis le début de la guerre a donc fait de la sécurité dans cette zone une priorité pour l'OTAN.

3. L'OTAN ET LA PROTECTION DES INFRASTRUCTURES SOUS-MARINES CRITIQUES

D'une manière générale, la protection des infrastructures sous-marines essentielles pour l'OTAN est encadrée par plusieurs articles de son traité fondateur. Plus précisément, l'article 2 sur la collaboration économique, l'article 3 sur la résilience et l'article 5 sur la défense collective du traité de l'Atlantique Nord (1949). En ce qui concerne ce dernier, le nouveau concept stratégique de l'OTAN (2022) mentionne les menaces hybrides qui pèsent sur les infrastructures critiques, réaffirmant leur inclusion dans le cadre de l'article susmentionné et soulignant l'engagement en faveur de la coopération internationale pour leur protection.

La préoccupation croissante pour la protection de ces infrastructures a fait de leur sécurité un objectif particulièrement important pour l'OTAN. Compte tenu de leur importance pour le fonctionnement de la société, des menaces telles que le contrôle acquis par des entreprises chinoises sur certaines de ces infrastructures et l'activité croissante de la Russie à proximité de celles-ci ont amené l'Alliance atlantique à se pencher sur l'état de ses infrastructures critiques en 2020 (García Pérez, 2023, p. 3).

Sur ce dernier point, le secrétaire général de l'OTAN de l'époque, Jens Stoltenberg (2020), a souligné l'importance des infrastructures sous-marines essentielles dans les efforts déployés par l'Alliance pour renforcer sa résilience :

Je pense qu'il est important d'aborder cette question, parce qu'il est important de comprendre que la plupart de ces câbles appartiennent à des propriétaires privés et que leur emplacement est connu du public. Cela les rend potentiellement vulnérables. Nous devons donc surveiller les vulnérabilités potentielles. C'est en partie la raison pour laquelle nous avons produit ce rapport. Nous disposons d'outils pour les protéger et pour surveiller les menaces. Nous avons également établi un nouveau commandement atlantique à Norfolk, un nouveau commandement de l'OTAN à Norfolk. L'une des tâches de ce nouveau commandement de l'Atlantique Nord est d'examiner comment protéger et surveiller les menaces qui pèsent sur les infrastructures sous-marines. Par exemple, Internet dépend de ces câbles, ce qui souligne l'importance des câbles sous-marins. L'un des principaux thèmes abordés lors de la réunion d'aujourd'hui était la résilience, qui concerne les infrastructures civiles, les services de santé et

les télécommunications. Mais, bien sûr, dans le cadre de nos efforts pour renforcer la résilience, les câbles sous-marins, l'infrastructure sous-marine est un élément important.

Toutefois, les principales mesures visant à protéger ces infrastructures ont été adoptées après le début de la guerre à grande échelle en Ukraine en 2022. Jusqu'alors, cette question faisait partie du travail d'institutions limitées, principalement liées au domaine maritime ou à la lutte contre les menaces hybrides, deux d'entre elles étant particulièrement remarquables.

D'une part, l'*Engagement de résilience renforcée*, créé en 2021 par une décision des chefs d'État et de gouvernement de l'OTAN, qui reconnaît l'engagement de l'Alliance à intensifier les efforts pour assurer la résilience de ses infrastructures critiques (OTAN, 2021). D'autre part, le *Comité de résilience de l'OTAN*, un organe responsable de la direction politique et stratégique, de l'orientation, de la planification et de la coordination générale des activités de résilience au sein de l'Alliance atlantique (OTAN, 2022) (voir le tableau 1).

Tableau 1

Les institutions de l'OTAN dans lesquelles la protection des infrastructures critiques a été encadrée avant la guerre à grande échelle en Ukraine en 2022.

Principales institutions	
2006	<i>Centre d'expédition de l'OTAN (NSC)</i>
2007	<i>Centre d'excellence pour la coopération civilo-militaire (CCOE)</i>
2008	<i>Centre d'excellence en coopération pour la cyberdéfense (CCD COE)</i>
2012	<i>Commandement maritime allié de l'OTAN (MARCOM)</i>
	<i>Centre d'excellence multinational pour la sécurité maritime (MARSEC COE)</i>
2014	<i>Centre d'excellence en communication stratégique</i>
2018	<i>Équipes de soutien à la lutte contre les armes hybrides</i>
2021	<i>Renforcement de l'engagement en faveur de la résilience</i>
2022	<i>Comité de résilience de l'OTAN</i>

Source : Élaboration propre sur la base des informations fournies par l'OTAN sur ses sites web.

En réponse au sabotage apparent du Nord Stream à la fin de 2022, l'OTAN a créé la *Cellule de coordination des infrastructures sous-marines critiques* (OTAN, 2023a) en février 2023. Un mois avant l'adoption de cette mesure, le 11 janvier 2023, la création d'un groupe de travail OTAN-UE sur la résilience des infrastructures critiques a été annoncée dans le cadre du dialogue structuré OTAN-UE existant sur la résilience, dans lequel il s'inscrit (Commission européenne & OTAN, 2023, p. 2).

Dans leur rapport publié en juin 2023, les deux parties soulignent l'existence d'une variété de menaces à affronter, allant d'éventuelles attaques terroristes à des catastrophes naturelles. Cependant, elles soulignent directement que depuis l'agression russe en Ukraine, ces infrastructures sont devenues un actif vulnérable dont la protection doit être une priorité (Commission européenne & OTAN, 2023, p. 4).

La création du *Centre maritime de l'OTAN pour la sécurité des infrastructures sous-marines critiques* (NMCSCUI) lors du sommet de Vilnius en 2023 est un autre exemple des effets de l'incident du Nord Stream en tant que tournant pour le renforcement des efforts occidentaux en matière de résilience de ses infrastructures sous-marines critiques :

La menace qui pèse sur les infrastructures sous-marines essentielles est réelle et se développe. Nous sommes déterminés à recenser et à atténuer les vulnérabilités et les dépendances stratégiques en ce qui concerne nos infrastructures essentielles, ainsi qu'à nous préparer, à dissuader et à nous défendre contre l'utilisation coercitive de l'énergie et d'autres tactiques hybrides par des acteurs étatiques et non étatiques. Toute attaque délibérée contre les infrastructures critiques des Alliés fera l'objet d'une réponse unie et déterminée ; cela s'applique également aux infrastructures sous-marines critiques. La protection des infrastructures sous-marines essentielles situées sur le territoire des Alliés demeure une responsabilité nationale, ainsi qu'un engagement collectif. L'OTAN se tient prête à soutenir les Alliés si et quand ils le demandent. Nous avons décidé de créer le Centre maritime de l'OTAN pour la sécurité des infrastructures sous-marines essentielles au sein du Commandement maritime de l'OTAN (MARCOM), ainsi qu'un réseau réunissant l'OTAN, les Alliés, le secteur privé et d'autres acteurs concernés, afin d'améliorer le partage des informations et d'échanger les meilleures pratiques (OTAN, 2023b).

Conformément à Stoltenberg (2020) et au rapport conjoint de la Commission européenne et de l'OTAN (2023, p. 3), le communiqué du sommet de Vilnius réaffirme l'inquiétude croissante de l'Alliance face aux menaces qui pèsent sur les infrastructures sous-marines essentielles. Dans cet extrait, l'OTAN reconnaît la nécessité d'identifier les vulnérabilités de manière proactive, souligne que ces menaces peuvent émaner d'acteurs étatiques et non étatiques et insiste sur l'importance d'une coordination efficace avec les acteurs concernés, en particulier ceux du secteur privé. Elle envisage aussi explicitement la possibilité que des attaques hybrides contre ces infrastructures puissent être considérées comme des actes justifiant l'activation de l'article 5 du traité de l'Atlantique Nord sur la défense collective.

Le NMCSCUI a donc été inauguré en mai 2024. L'OTAN le définit comme un réseau et un centre de connaissances spécialisé dans les infrastructures sous-marines critiques, dont la fonction principale est de soutenir les processus de décision stratégique, de faciliter le déploiement opérationnel des forces et de coordonner les actions conjointes pour assurer leur protection. Cela se fait par l'intégration des efforts entre les États membres, les partenaires stratégiques et le secteur privé (NATO Media Centre, 2024).

Ce n'est toutefois pas la seule mesure issue du sommet de Vilnius mise en œuvre par l'OTAN pour garantir une meilleure prise en compte des menaces dans le domaine maritime. En octobre 2023, la *Vision numérique des océans*, une initiative visant à améliorer la compréhension du domaine maritime en harmonisant davantage les capacités nationales et alliées de surveillance maritime utilisant une gamme diversifiée de moyens, a été adoptée (OTAN, 2023c).

De plus, face aux défis croissants de ces infrastructures, l'OTAN a organisé le 23 mai 2024 la première réunion du réseau d'infrastructures sous-marines critiques sur

décision des ministres de la défense dans le but d'améliorer la coordination et l'échange d'informations. Cette réunion a permis d'examiner des mesures telles que le renforcement des patrouilles navales, la promotion de l'innovation technologique et l'utilisation de capacités de détection et de réaction avancées, consolidant ainsi le rôle central de l'Alliance dans ce domaine (OTAN, 2024b).

En novembre 2024, l'exercice *Bold Machina 24* a été mené à La Spezia, en Italie, sous la coordination du *Commandement des forces d'opérations spéciales alliées* (SOFCOM) et du *Centre de recherche et d'expérimentation maritimes* (CMRE), dans le but de tester des capteurs sous-marins pour la protection des infrastructures critiques (Centre OTAN de recherche et d'expérimentation maritimes, 2024, p. 2). Ces exercices reflètent l'intérêt susmentionné pour l'intégration des technologies émergentes, telles que les systèmes sans pilote, afin de renforcer la sécurité dans le domaine sous-marin (Conte de los Ríos, 2025, p. 26).

À cet égard, il convient également de noter que l'OTAN a mis au point de nouveaux outils qui permettent aux alliés de détecter les activités suspectes afin de se protéger contre le sabotage. Ces outils comprennent l'utilisation de l'intelligence artificielle, comme le montre *Mainsail*, un logiciel développé par le CCRE qui détecte les navires ayant un comportement suspect dans l'intention de recueillir des informations sur les infrastructures sous-marines et de les endommager (NATO Multimedia, 2025).

En ce qui concerne la protection spécifique des infrastructures sous-marines de la mer Baltique, l'OTAN a encouragé l'innovation technologique nécessaire à la détection efficace de toute activité suspecte pour compléter le travail de ses patrouilles dans la région. Ces mesures ont été progressivement intensifiées en conséquence directe du sabotage apparent du Nord Stream, comme le reconnaît l'Alliance elle-même (OTAN, 2023d).

En février 2025, l'OTAN a procédé à une démonstration de véhicules de surface sans pilote (USV) en mer Baltique afin de faire progresser leur intégration opérationnelle dans les tâches de surveillance maritime. Cette initiative s'inscrit dans le cadre des efforts déployés par l'Alliance pour intégrer des technologies émergentes et perturbatrices - telles que les systèmes autonomes et l'intelligence artificielle - visant à optimiser la connaissance de la situation et à renforcer la protection des infrastructures sous-marines essentielles, en particulier le long des lignes de communication maritimes (Commandement allié maritime de l'OTAN, 2025b). En outre, dans le cadre du Comité sur la résilience, l'OTAN a présenté son premier *programme de référence sur la résilience* en 2025, dans le but de renforcer les capacités des alliés face aux menaces, y compris celles qui visent les infrastructures critiques (OTAN, 2025a).

Parallèlement, la coopération avec l'Union européenne a gagné en importance grâce à des initiatives telles que la *boîte à outils hybride de l'UE*, la *cellule de fusion hybride* et les *équipes de réaction rapide hybride*, conçues pour promouvoir les synergies et renforcer la coordination anti-hybride avec l'OTAN (Service européen pour l'action extérieure, 2022, p. 34). Cette convergence d'initiatives entre les entités susmentionnées démontre l'importance de développer des capacités défensives solides, et leur mise en œuvre coordonnée ainsi que l'intégration efficace des nouvelles technologies et capacités opérationnelles sont essentielles pour assurer une protection efficace des infrastructures

sous-marines européennes, en particulier au vu de l'évolution rapide des menaces affectant ce domaine (Conte de los Ríos, 2025, p. 33).

Enfin, il convient de noter que l'OTAN considère le renforcement de la coopération avec le secteur privé comme une dimension essentielle de l'amélioration de sa capacité à répondre aux menaces qui pèsent sur les infrastructures sous-marines essentielles. Cette coopération se justifie, d'une part, par le fait qu'une part importante de ces infrastructures est détenue ou exploitée par le secteur privé et, d'autre part, par le potentiel du secteur privé à fournir des solutions technologiques essentielles dans un environnement opérationnel de plus en plus complexe (Fridbertsson, 2023, p. 11).

4. OPÉRATION BALTIC SENTRY

Le 14 janvier 2025, l'OTAN a tenu un sommet des Alliés de la mer Baltique pour faire face aux menaces croissantes qui pèsent sur les infrastructures sous-marines essentielles de la région. À l'issue de ce *sommet*, le secrétaire général de l'Alliance atlantique et les participants ont publié la *déclaration conjointe du sommet des Alliés de l'OTAN sur la mer Baltique* (2025) annonçant le lancement d'une initiative militaire visant à renforcer la protection de ces infrastructures : l'opération *Baltic Sentry*.

Se déclarant profondément préoccupée par l'augmentation des actions qui menacent le fonctionnement des infrastructures sous-marines essentielles, l'Alliance a indiqué qu'elle était prête à "dissuader, détecter et contrer toute tentative de sabotage" et à répondre à toute attaque "par une réaction ferme et décisive" (Tasavallan Presidentti, 2025). Cela intervient à un moment où l'OTAN reconnaît la nécessité de moderniser ses capacités pour renforcer sa dissuasion et sa défense afin de faire face et de contrer l'évolution des menaces pour la sécurité (Tasavallan Presidentti, 2025).

Le MARCOM, sous la direction du *Commandement des forces interarmées de Brunssum* (JFCBS), est reconnu comme jouant un rôle clé dans la coordination des opérations dans le cadre de ce qu'il définit comme une "activité de surveillance multi-domaine visant à accroître la connaissance de la situation maritime en mer Baltique afin de dissuader les attaques contre les infrastructures sous-marines essentielles et de s'en défendre" (Commandement maritime allié de l'OTAN, 2025a). À cette fin, l'opération *Baltic Sentry* prévoit le déploiement par les alliés de moyens maritimes, aériens et terrestres supplémentaires pour renforcer la surveillance et la dissuasion.

En organisant régulièrement des patrouilles et des exercices conjoints, l'OTAN cherche à maintenir une présence constante en mer Baltique, qui est surveillée en permanence par des navires de guerre, des sous-marins, des aéronefs et des technologies de pointe en matière de surveillance maritime. Par exemple, des navires du *1er groupe maritime permanent OTAN* (SNMG1) et du *1er groupe permanent OTAN de lutte contre les mines* (SNMCMG1) participeront à *Baltic Sentry* aux côtés d'autres navires de patrouille maritime alliés, tandis que l'OTAN continuera d'investir dans des technologies militaires de pointe pour détecter et minimiser les menaces, telles que l'intelligence artificielle, les capteurs avancés et les systèmes de sonar spécialisés (MARCOM, 2025).

À cela s'ajoute l'inclusion de deux acteurs clés au sein de l'Alliance. D'une part, la *Force opérationnelle du commandant* (CTF) en mer Baltique, récemment inaugurée et basée dans la ville portuaire de Rostock. Outre la coordination des navires alliés dans la

mer Baltique, la CTF s'efforce d'élaborer une vision régionale unifiée des infrastructures critiques dans la mer Baltique afin de soutenir les efforts de protection stratégique de l'OTAN (Tasavallan Presidentti, 2025). D'autre part, le NMCSCUI susmentionné concentrera ses efforts sur la protection et la sécurisation des actifs sous-marins vitaux (Tasavallan Presidentti, 2025).

Pour atteindre ces objectifs, l'OTAN considère qu'il est essentiel non seulement de travailler au sein de l'Alliance elle-même, mais aussi de collaborer et de coopérer avec d'autres acteurs allant de l'UE au secteur privé. Alors que dans le premier cas, la coopération se concentrera sur le renforcement des mécanismes existants, dans le cas du secteur privé, l'OTAN souligne l'importance de coopérer avec les opérateurs d'infrastructures et les entreprises de technologie de pointe pour développer les différentes mesures de réponse nécessaires pour accroître la résilience (Tasavallan Presidentti, 2025).

L'Alliance atlantique envisage également l'adoption de nouvelles mesures conformes au droit international, visant à la fois la prévention et la réponse aux menaces ou aux actes irresponsables contre les infrastructures sous-marines critiques dans la région (Tasavallan Presidentti, 2025). Dans le cadre du lancement de l'opération *Baltic Sentry*, l'actuel secrétaire général de l'OTAN, Mark Rutte, a souligné la nécessité d'une application stricte du cadre juridique existant, avertissant que toute menace potentielle contre ces infrastructures pourrait conduire à des mesures coercitives telles que l'arraisonnement, la saisie ou la détention de navires. Dans ce contexte, il a cité la réponse de la Finlande aux incidents comme un exemple remarquable d'action (OTAN, 2025b).

La mise en œuvre de ces mesures est justifiée par la mention constante de l'existence de menaces. En ce qui concerne ces dernières, une menace en particulier est mentionnée, celle de la "flotte fantôme russe". Celle-ci est définie comme une menace importante pour la sécurité maritime et environnementale, tant dans la région de la mer Baltique qu'au niveau mondial, car elle compromet l'intégrité des infrastructures sous-marines, augmente les risques liés aux munitions chimiques déversées sur les fonds marins et représente une source majeure de financement de la guerre d'agression illégale de la Russie contre l'Ukraine (Tasavallan Presidentti, 2025).

De même, il est reconnu que la menace qui pèse sur les infrastructures sous-marines essentielles ne se limite pas à la mer Baltique. Elle souligne donc que l'opération *Baltic Sentry* représente également un tournant en faveur d'une plus grande coopération pour renforcer la résilience de ces infrastructures critiques et, par conséquent, pour renforcer la sécurité de l'OTAN. Ainsi, le lancement de l'opération elle-même va de pair avec l'annonce du renouvellement de la stratégie maritime de l'alliance (Tasavallan Presidentti, 2025).

5. CONCLUSIONS ET PROPOSITIONS

Les infrastructures sous-marines critiques sont vitales pour l'économie et le système de communication mondial. Leur importance croissante et les progrès technologiques constants dans ce domaine en ont fait une cible prioritaire pour la défense, mais aussi pour d'éventuelles attaques. Ainsi, *la guerre des fonds marins* n'est plus un concept lointain, mais une menace immédiate pour les Alliés. Le lien étroit entre la sécurité de ces infrastructures et la stabilité mondiale, notamment en termes économiques et de

communication, fait que leur protection et la gestion de leurs vulnérabilités constituent désormais une priorité de défense pour tous les acteurs internationaux.

Dans le contexte actuel de rivalité avec une Russie qui annonce publiquement sa volonté de déstabiliser l'OTAN, la mise en œuvre de stratégies de protection des infrastructures critiques devient un objectif extrêmement urgent pour la défense de l'Alliance atlantique, en particulier dans la région de la Baltique. Comme mentionné dans le document, la mer Baltique n'est pas seulement une enclave de compétition géopolitique entre l'OTAN et la Russie, mais aussi une zone clé pour la sécurité des infrastructures sous-marines critiques qui garantissent la stabilité des Alliés. Unir ses forces dans cette région pour renforcer sa sécurité doit donc être une priorité pour l'OTAN, surtout depuis la guerre de 2022 en Ukraine et l'adhésion de la Suède et de la Finlande à l'Alliance.

Cela nous permet de tirer la principale conclusion liée à l'objectif spécifique numéro un de cette étude. Alors que la protection de ces infrastructures devrait déjà être un objectif pour l'OTAN compte tenu de leur importance pour la résilience de la société et de leur extrême vulnérabilité à un large éventail de menaces, la situation géopolitique actuelle fait de ces infrastructures une cible évidente pour d'éventuelles attaques. En témoigne l'augmentation des incidents impliquant des câbles sous-marins dans la mer Baltique depuis le début du conflit en 2022, avec huit incidents à ce jour au cours desquels des infrastructures critiques de la région ont été endommagées, pratiquement tous survenus dans la ZEE de la Finlande et de la Suède, pays qui, par coïncidence, ont demandé à adhérer à l'OTAN la même année en dépit de l'opposition farouche du Kremlin (voir tableau 2).

Tableau 2
Incidents survenus dans les infrastructures sous-marines critiques de la mer Baltique depuis 2022.

	Infrastructure	Lieu de l'incident	Pays concernés	Causes
Nord Stream	Conduite sous-marine	ZEE suédoise et danoise	Union européenne	Nombreuses indications de sabotage
Balticconnector	Conduite sous-marine	ZEE finlandaise	Finlande et Estonie	Nombreuses indications de sabotage
C-Lion 1	Câble de télécommunications	ZEE suédoise	Finlande et Allemagne	Nombreuses indications de sabotage
Liaison est-ouest BCS	Câble de télécommunication	ZEE suédoise	Lituanie et Suède	Nombreuses indications de sabotage
GlobalConnect	Câbles de télécommunication	ZEE finlandaise	Finlande et Suède	Accident
Estlink 2	Réseau électrique	ZEE suédoise	Finlande et Estonie	Nombreuses indications de sabotage
Centre national de radio et de	Câble de télécommunications	ZEE suédoise	Suède et Lettonie	Accident

**télévision de
Lettonie**

Gotland	Câble maritime appartenant à une société finlandaise	ZEE suédoise	Finlande et Allemagne	Nombreuses indications de sabotage
----------------	--	--------------	-----------------------	------------------------------------

Source : Élaboration propre

En ce qui concerne le deuxième objectif spécifique de cette étude sur le cadre d'action global de l'OTAN pour la protection des infrastructures sous-marines critiques, plusieurs conclusions peuvent être tirées. Malgré l'attrition des performances de l'armée russe dans la guerre d'Ukraine et les graves revers subis dans le domaine naval, les tactiques hybrides russes restent la menace la plus pressante pour les infrastructures européennes dans la mer Baltique. L'OTAN se positionne comme un acteur central dans la prévention des attaques contre ces infrastructures, en intensifiant ses efforts par des mesures progressives à partir de 2022 à la suite de l'invasion de l'Ukraine et des incidents qui ont suivi.

Alors que cette question faisait partie des travaux d'institutions essentiellement maritimes, l'OTAN a adopté près d'une douzaine de mesures depuis l'apparent sabotage du Nord Stream, en pleine période de tensions avec Moscou. Il s'agit notamment de la création de la *cellule de coordination des infrastructures sous-marines critiques* ou du *centre maritime de l'OTAN pour la sécurité des infrastructures sous-marines critiques*, de l'initiative *Digital Ocean Vision*, d'exercices militaires tels que *Bold Machina 24*, de l'innovation technologique nécessaire pour tirer parti de l'intelligence artificielle telle que *Mainsail*, et de l'adoption d'initiatives complémentaires avec des acteurs tiers tels que l'Union européenne.

L'opération *Baltic Sentry* est la principale réponse de l'OTAN au défi que représentent la protection des infrastructures sous-marines essentielles en mer Baltique et le renforcement de la sécurité dans la région. Conformément à l'objectif principal de l'étude axée sur l'analyse de cette opération, on peut observer que les mesures mises en œuvre dans son cadre visent à renforcer les capacités de détection, de dissuasion-prévention, d'adaptation et de réaction, ce qui est conforme aux principaux critères proposés par la littérature spécialisée pour l'adoption d'une stratégie efficace (voir le tableau 3).

Tableau 3

Mise en œuvre des éléments nécessaires à une stratégie efficace de protection des infrastructures sous-marines critiques dans le cadre de l'opération Baltic Sentry de l'OTAN.

Opération OTAN Baltic Sentry	
Présence ou surveillance accrue	✓
Collaboration avec les acteurs internationaux	✓
Coordination avec le secteur privé	✓
Utilisation de technologies avancées	✓
Élaboration de cadres réglementaires	✓
Renouvellement de la stratégie maritime	✓
Mise en œuvre des mesures d'intervention	✓

Source : Élaboration propre sur la base de Conte de los Ríos (2025), Monaghan et al. (2023), Fridbertsson (2023) et des informations fournies par l'OTAN.

En bref, l'opération *Baltic Sentry* démontre que les infrastructures sous-marines critiques sont actuellement identifiées par l'OTAN comme une vulnérabilité stratégique dont la protection est essentielle pour assurer la résilience et la sécurité non seulement de l'Alliance, mais aussi de la vie quotidienne de la société. Une leçon qui trouve un tournant dans les différents épisodes survenus dans le cadre de la guerre en Ukraine depuis 2022, l'attaque apparente contre Nord Stream à la fin de la même année étant remarquable, comme le montre à la fois le cadre chronologique des mesures adoptées par l'OTAN dans ce secteur et l'Alliance elle-même lorsqu'elle justifie ces dernières.

Ainsi, pour répondre à la question générale de la recherche, l'hypothèse générale de l'étude est que l'opération *Baltic Sentry* renforce la protection des infrastructures sous-marines essentielles dans la mer Baltique et la présence de l'Alliance dans la mer Baltique, s'adaptant ainsi au nouveau contexte de menace.

RÉFÉRENCES BIBLIOGRAPHIQUES

- Arjona Hernández, N. (2023). La protection des câbles de télécommunications sous-marins : Digital sovereignties and submarine cable network security. *International Journal Of Policy Thinking*, 18(18), pp. 41-67. <https://doi.org/10.46661/revintpensampolit.8753>
- Commission de protection de l'environnement marin de la Baltique (2024). *HELCOM Map and Data Service*. <https://maps.helcom.fi/website/mapservice/>
- Commission de protection de l'environnement marin de la Baltique (2024). *HELCOM Map and Data Service*. <https://maps.helcom.fi/website/mapservice/>
- Birnbaum, M. (22 décembre 2017). Les sous-marins russes rôdent autour de câbles sous-marins vitaux. Cela rend l'OTAN nerveuse. *The Washington Post*. https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?hpid=hp_hp-top-table-main_russiasubs712pm%3Ahomepage%2Fstory
- Bueger, C., Liebetrau, T., et Franken, J. (2022). *Menaces pour la sécurité des câbles et des infrastructures de communication sous-marins - Conséquences pour l'UE*. Analyse approfondie du Parlement européen, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)
- Bueger, C. et Liebetrau, T. (2021). Protecting hidden infrastructure : The security politics of the global submarine data cable network (Protéger une infrastructure cachée : la politique de sécurité du réseau mondial de câbles de données sous-marins). *Contemporary Security Policy*, 42(3), pp. 391-413. <https://doi.org/10.1080/13523260.2021.1907129>
- Cassetta, M. (2024). Comment répondre aux nouvelles menaces qui pèsent sur les infrastructures sous-marines essentielles à l'heure de la guerre de la Russie contre l'Ukraine. *Istituto Affari Internazionali (IAI), IAI Commentaries 24-31 juin 2024*, pp. 1-5. <https://www.iai.it/en/pubblicazioni/c05/how-respond-emerging-threats-critical-underwater-infrastructure>
- Childs, N. (2025). La "flotte fantôme" de la Russie et l'évasion des sanctions : que faire ? *The International Institute for Strategic Studies (IISS)*, janvier 2025, pp. 1-15. https://www.iiiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf
- Cinia (20 février 2025). *Perturbation du câble sous-marin C-Lion de Cinia*. <https://www.cinia.fi/en/news/disturbance-in-cinia-c-lion-submarine-cable>

- Cinia (n.d.). *Connectivité internationale par Cinia*.
<https://www.cinia.fi/hubfs/Cinia%20Theme%202024/Muut%20kuvat/Cinian-kansainvaliset-verkkoyhteydet-kartta.jpg>
- Clark, B. (2015). *L'ère émergente de la guerre sous-marine*. Center for Strategic and Budgetary Assessments (CSBA),
<https://csbaonline.org/research/publications/undersea-warfare>.
- Conte de los Ríos, A. (2025). Menaces pour la sécurité : fonds marins et infrastructures critiques. *Global Affairs Journal*, (7), pp. 26-35.
<https://www.unav.edu/documents/16800098/147587031/amenazas-seguridad.pdf>
- Deni, J. R. (18 décembre 2023). *La mer Baltique est-elle un lac de l'OTAN ?* Carnegie Endowment for International Peace.
<https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake?lang=en>
- Energistytrelsen (26 septembre 2022). *Fuite du North Stream 2 dans la mer Baltique*.
<https://ens.dk/en/press/leak-north-stream-2-baltic-sea>
- Commission européenne et OTAN . (2023). *TASK OF FORCE UE-OTAN SUR LA RÉSILIENCE DES INFRASTRUCTURES CRITIQUES. RAPPORT D'ÉVALUATION FINAL*. https://www.nato.int/cps/en/natohq/news_216631.htm
- Service européen pour l'action extérieure (2022). *UN COMPAS STRATÉGIQUE POUR LA SÉCURITÉ ET LA DÉFENSE : Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts et qui contribue à la paix et à la sécurité internationales*.
https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
- Fingrid (s.d.). *EstLink 2 - deuxième liaison de courant continu à haute tension entre la Finlande et l'Estonie*. <https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/>
- Fink, A. et Kofman, M. (2020). La stratégie russe de gestion de l'escalade : débats et acteurs clés de la pensée militaire. *Note d'information de l'ANC, avril 2020*, p. 1-48. https://www.cna.org/cna_files/pdf/DIM-2020-U-026101-Final.pdf
- Foggo, J. (17 janvier 2023). La quatrième bataille de l'Atlantique est en cours. *Centre d'analyse des politiques européennes (CEPA)*, <https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/>
- Foggo, J. et Fritz, A. (2016). La quatrième bataille de l'Atlantique. *U.S. Naval Institute*, 142(6), <https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic>
- Forsvaret. [@forsvaretdk] (20 novembre 2024). *Concernant le navire chinois Yi Peng 3 : La Défense danoise peut confirmer que nous sommes présents dans la zone*

proche du navire chinois Yi Peng 3. La Défense danoise n'a pas d'autres commentaires à faire pour le moment. [Post in X]. X. <https://x.com/forsvaretdk/status/1859195509866381402>

Fridbertsson, N. T. (2023). *Protection des infrastructures maritimes essentielles - Le rôle de la technologie*. Rapport général. 032 STC 23 E. Assemblée parlementaire de l'OTAN : Commission de la science et de la technologie (STC). <https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc>

García Pérez, R. (2023). L'Espagne dans le réseau mondial de câbles sous-marins. *Instituto Español de Estudios Estratégicos, IEEE Framework Document 10/2023*, pp. 1-51. <https://www.defensa.gob.es/ceseden/-/espa%C3%B1a-en-la-red-global-de-cables-submarinos>

García Pérez, R. (2024). "La seguridad de los cables submarinos", in Fernando Ibáñez Gómez (Coord.), *Seguridad marítima. Una incertidumbre permanente*, Bosch Editor, Barcelona, pp. 265-298.

Gasgrid (n.d.). *Carte des transmissions de gaz finlandaises et baltiques*. https://gasgrid.fi/wp-content/uploads/Gasgrid_maakaasu_lisaversiot_eu_EN-scaled.jpg

Gasum (2023). *Gasum a résilié son contrat de fourniture de gaz naturel par gazoduc avec Gazprom Export*. <https://www.gasum.com/en/news-and-customer-stories/news-and-press-releases/2023/gasum-has-terminated-its-pipeline-natural-gas-supply-contract-with-gazprom-export/#:~:text=The%20parties%20were%20not%20able,details%20of%20the%20contract%20termination.>

Gresh, G. F. (2023). *Europe's new maritime security reality : Chinese ports, Russian bases, and the rise of subsea warfare (La nouvelle réalité de la sécurité maritime de l'Europe : les ports chinois, les bases russes et la montée de la guerre sous-marine)*. Foreign Policy at Brookings, Policy Brief, février 2023. <https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/>

Guilfoyle, D., Paige, T. P., et McLaughlin, R. (2022). THE FINAL FRONTIER OF CYBERSPACE : THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES. *International and Comparative Law Quarterly*, 71(3), pp. 657-696. <https://doi.org/10.1017/S0020589322000227>

Groupe Insikt (2023). *The Escalating Global Risk Environment for Submarine Cables*. Recorded Future Threat Analysis, <https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables>

- Comité international de protection des câbles (2024). *Rapport du Comité international de protection des câbles Docs : HSSC16-07.10A : Activités de l'ICPC affectant le HSSC*. Organisation hydrographique internationale, Tokyo, Japon, 27-31 mai 2024.
https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf
- Jones, S. G. (2025). Russia's Shadow War Against the West (La guerre de l'ombre de la Russie contre l'Occident). *Center for Strategic and International Studies (CSIS), CSIS Briefs March 2025*, pp. 1-20. <https://www.csis.org/analysis/russias-shadow-war-against-west>
- Kaushal, S. (25 mai 2023). *La traque des fonds marins : How Russia Targets Critical Undersea Infrastructure*. Royal United Services Institute (RUSI), mai 2023.
<https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure>
- Kieler Nachrichten (2025). *Verdacht der Sabotage : Ermittler suchen Anker vom russischen Frachter "Arne"* [Soupçon de sabotage : les enquêteurs recherchent l'ancre du cargo russe "Arne"]. <https://www.kn-online.de/schleswig-holstein/verdacht-der-sabotage-gegen-russischen-frachter-arne-in-kiel-ermittlungsstand-ORSQRUDZZRGJHC7KSCB4SKJCDM.html>
- Centre national de radio et de télévision de Lettonie (2025). *Le câble sous-marin à fibre optique de LVRTC a été endommagé*. <https://www.lvrtc.lv/en/news/jaunumi/lvrtc-submarine-optical-fiber-cable-damaged/>
- Latvijas Vēstnesis (28 juillet 2022). *Grozījumi Enerģētikas likumā* [Amendements à la loi sur l'énergie]. <https://www.vestnesis.lv/op/2022/144.5>
- Lietuvos Respublikos Energetikos Ministerija (20 mai 2022). *Plus d'importations de pétrole, de gaz et d'électricité russes en Lituanie à partir de dimanche*. <https://enmin.lrv.lt/en/news/no-more-russian-oil-gas-and-electricity-imports-in-lithuania-from-sunday/>
- LRT TV (18 novembre 2024). *Le câble sous-marin entre la Lituanie et la Suède est endommagé - Telia*. https://www.lrt.lt/en/news-in-english/19/2416006/undersea-cable-between-lithuania-and-sweden-damaged-telia?srsltid=AfmBOoowPquC_SbY0w-dUT2dfxJTzPrj-OPvif6IxXoDTJQuKnQx11fF
- McNamara, E. M. (17 mars 2016). *Sécuriser la région nordique et balte*. Revue de l'OTAN. <https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html>
- McNamara, E. M. (28 août 2024). *Renforcer la résilience : le rôle de l'OTAN dans l'amélioration de la sécurité des infrastructures sous-marines essentielles*. Revue de l'OTAN : opinions, analyses et débats sur les questions de sécurité, <https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html>

Ministère des affaires étrangères de Finlande (18 novembre 2024). *Déclaration conjointe des ministres des Affaires étrangères de Finlande et d'Allemagne sur le câble sous-marin rompu en mer Baltique*. https://um.fi/statements/-/asset_publisher/6zHpMjnoIHgI/content/joint-statement-by-the-foreign-ministers-of-finland-and-germany-on-the-severed-undersea-cable-in-the-baltic-sea/35732

Ministère des affaires économiques et de l'emploi de Finlande (7 mai 2024). *Hallituksen esitys laiksi laiksi maakaasun ja nesteytetyn maakaasun maahantuonnin väliaikaisesta kieltämisestä Venäjän federaatiosta ja Valko-Venäjältä* [Proposition de loi du gouvernement sur l'interdiction temporaire des importations de gaz naturel et de gaz naturel liquéfié en provenance de la Fédération de Russie et du Belarus]. <https://tem.fi/en/project?tunnus=TEM036:00/2024>

Monaghan, S. (6 octobre 2022). Cinq mesures que l'OTAN devrait prendre après l'attaque du gazoduc Nord Stream. *Centre d'études stratégiques et internationales (CSIS)*, <https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack>

Commandement maritime allié de l'OTAN (2025a, 14 janvier 2025). *La Baltic Sentry de l'OTAN intensifie ses patrouilles en mer Baltique pour protéger les infrastructures sous-marines essentielles*. <https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure>

Commandement maritime allié de l'OTAN (2025b, 20 février 2025). *L'OTAN effectue une démonstration de véhicule de surface sans pilote en mer Baltique*. <https://mc.nato.int/media-centre/news/2025/page228602539>

Centre OTAN de recherche et d'expérimentation maritimes (2024). *BULLETIN D'INFORMATION DU CENTRE DE RECHERCHE MARITIME DE L'OTAN*. January-June 2024. [https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20\(002\).pdf](https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20(002).pdf)

Centre des médias de l'OTAN (2024, 28 mai 2024). *L'OTAN lance officiellement le nouveau Centre maritime pour la sécurité des infrastructures sous-marines essentielles*. <https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui>

OTAN Multimédia (06 février 2025). *Protéger les câbles sous-marins grâce à l'intelligence artificielle*. <https://www.natomultimedia.tv/app/asset/718197>

OTAN (2021, 14 juin 2021). *Engagement de résilience renforcée*. https://www.nato.int/cps/en/natohq/official_texts_185340.htm

OTAN (2022, 07 octobre 2022). *Comité de résilience*. https://www.nato.int/cps/in/natohq/topics_50093.htm

- OTAN (2023a, 15 février 2023). *L'OTAN met en place une cellule de coordination de l'infrastructure sous-marine.* https://www.nato.int/cps/en/natohq/news_211919.htm
- OTAN (2023b, 11 juillet 2023). *Communiqué du Sommet de Vilnius. Publié par les chefs d'État et de gouvernement des pays de l'OTAN participant à la réunion du Conseil de l'Atlantique Nord tenue à Vilnius le 11 juillet 2023.* https://www.nato.int/cps/en/natohq/official_texts_217320.htm
- OTAN (2023c, 12 octobre 2023). *Les ministres de la Défense des pays de l'OTAN lancent une initiative visant à renforcer les capacités de surveillance maritime.* https://www.nato.int/cps/ra/natohq/news_219441.htm
- OTAN (2023d, 19 octobre 2023). *L'OTAN renforce les patrouilles en mer Baltique après l'endommagement d'infrastructures sous-marines.* https://www.nato.int/cps/en/natohq/news_219500.htm
- OTAN (2024a, 30 décembre 2024). *L'OTAN va renforcer sa présence militaire en mer Baltique.* https://www.nato.int/cps/en/natohq/news_231800.htm
- OTAN (2024b, 23 mai 2024). *L'OTAN tient la première réunion du réseau d'infrastructures sous-marines critiques.* https://www.nato.int/cps/en/natohq/news_225582.htm
- OTAN (2025a, 21 février 2025). *L'OTAN lance le programme de référence sur la résilience.* https://www.nato.int/cps/en/natohq/news_233458.htm
- OTAN (2025b, 14 janvier 2025). *L'OTAN lance la " Baltic Sentry " pour renforcer la sécurité des infrastructures critiques.* https://www.nato.int/cps/en/natohq/news_232122.htm
- Police de Finlande (2025b, 2 mars 2025). *Le pétrolier Eagle S doit passer dans les eaux internationales sous le contrôle des gardes-frontières.* <https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control>
- Police finlandaise (2023a, 24 octobre 2023). *Le Bureau national d'enquête a clarifié, sur le plan technique, la cause de l'endommagement du gazoduc.* <https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage>
- Police finlandaise (2023b, 17 octobre 2023). *Le Bureau national d'enquête examine les antécédents des navires naviguant dans la zone d'endommagement du gazoduc.* <https://poliisi.fi/en/-/national-bureau-of-investigation-examines-background-of-vessels-sailing-in-the-gas-pipeline-damage-area>
- Police de Finlande (2025a, 3 décembre 2025). *La police ne soupçonne aucune infraction pénale dans les deux incidents de dommages aux câbles dans le sud de la Finlande.* <https://poliisi.fi/en/-/police-do-not-suspect-any-criminal-offence-in-either-of-the-cable-damage-incidents-in-southern-finland>

Police de Finlande (2025c, 21 février 2025). *Le Bureau national d'enquête mènera une enquête préliminaire sur les dommages présumés causés aux câbles dans la mer Baltique.* <https://poliisi.fi/en/-/national-bureau-of-investigation-to-conduct-a-preliminary-inquiry-into-suspected-cable-damage-in-baltic-sea>

Politiet (31 janvier 2025). *Le navire peut quitter Tromsø.* <https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2025/01/31/troms2/>

Quijarro Santibáñez, L. (2023). Seabed Warfare : Submarine Warfare in the 21st Century (La guerre des fonds marins : la guerre sous-marine au XXIe siècle). *Revista de Marina*, 141(997), pp. 15-22. <https://revistamarina.cl/revista/997>

Région de Gotland (3 mars 2025). *Misstänkt sabotage* [Sabotage présumé]. <https://gotland.se/bygga-bo-och-miljo/vatten-och-avlopp/dricksvatten/misstankt-sabotage>

République d'Estonie Ministère des affaires étrangères . (2022). *L'Estonie interdit les importations et les achats de gaz naturel en provenance de Russie.* <https://www.vm.ee/en/news/estonia-imposes-ban-natural-gas-imports-and-purchases-russia>

Reuters (2024). *Câbles de fibre optique endommagés dans la mer Baltique.* <https://www.reuters.com/graphics/BALTICSEA-CABLES/zdpxqaaxwvx/chart.png>

Reuters (2025). *Câble à fibres optiques endommagé dans la mer Baltique.* <https://www.reuters.com/graphics/BALTIC-SECURITY/xmvjbdamavr/chart.png>

Stoltenberg, J. (22 octobre 2020). *Conférence de presse en ligne du secrétaire général de l'OTAN, Jens Stoltenberg, à l'issue de la première journée des réunions des ministres de la Défense de l'OTAN.* https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Forum des télécommunications sous-marines (2025). *Global Outlook.* SubTel Forum Magazine #140. <https://subtelforum.com/subtel-forum-magazine-140-global-outlook/>

Autorité suédoise des poursuites (2025). *Le procureur révoque la décision sur le navire saisi.* https://www.aklagare.se/en/media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/?_t_id=ajCngOfkVK4qcLdxSmm4EA%3d%3d&_t_uuid=ajbjBKKEs7uVHPgMJkVsvA&_t_q=baltic&_t_tags=language%3aen%2csiteid%3a764c28f6-3ce5-48e7-a8ec-b8f5f22e4245%2candquerymatch&_t_hit.id=Aklagare_Web_Business_PressReleases_Models_PressReleasePage/_847c0fdb-df1d-4d16-9b4a-0db494be3af4_fr&_t_hit.pos=2

Tasavallan Presidentti (14 janvier 2025). *Déclaration conjointe du Sommet des Alliés de l'OTAN sur la mer Baltique*. <https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/>

Agence spatiale européenne (06 octobre 2022). *Carte du gazoduc Nordstream avec le trafic maritime*. https://www.esa.int/ESA_Multimedia/Images/2022/10/Nordstream_pipeline_map_with_shipping_traffic

Yle (2024a, 31 décembre 2024). *Police : No crime suspected in Finland-Sweden cable break*. <https://yle.fi/a/74-20128835>

Yle (2024b). *Le câble a été endommagé en deux endroits distincts entre Espoo et Vihti. Image: Laura Merikalla / Yle, Mapcreator, OpenStreetMap, GlobalConnect*. https://images.cdn.yle.fi/image/upload/c_crop,h_1080,w_1919,x_0,y_0/ar_1.7777777777777777,c_fill,g_faces,h_675,w_1200/dpr_2.0/q_auto:eco/f_auto/fl_lossy/v1733216443/39-1389673674ec7f18a492

RÈGLEMENT

Convention des Nations unies sur le droit de la mer, New York, 30 avril 1982.
https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Convention pour la protection des câbles télégraphiques sous-marins, Paris, 14 mars 1884.
https://iscpc.org/information/Convention_on_Protection%20of_Cables_1884.pdf

Le nouveau concept stratégique de l'OTAN, Madrid, 29 juin 2022.
https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

Traité de l'Atlantique Nord, Washington, 4 avril 1949.
https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es



Article de recherche

LE CAPITAL INTELLECTUEL DANS L'INSTITUTION DE LA GARDE CIVILE ET SA CONTRIBUTION A L'ECONOMIE SOCIALE

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

Virginia Belén Subiris Moriel

Doctorant à l'université Rey Juan Carlos.

Programme de sciences sociales et juridiques. Secteur des affaires

Master Gestion internationale des ressources humaines

(Gestion des ressources humaines internationales)

virbelsu@gmail.com

ORCID: <https://orcid.org/0009-0000-2569-3710>

Reçu le 31/03/2025

Accepté le 10/06/2025

Publié le 27/06/2025

Citation recommandée : Subiris, V. (2025). Le capital intellectuel dans l'institution de la Guardia Civil et sa contribution à l'économie sociale. *Revista Logos Guardia Civil*, 3(2), p.p. 257-292.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

LE CAPITAL INTELLECTUEL DE LA GARDE CIVILE ET SA CONTRIBUTION A L'ECONOMIE SOCIALE

Résumé : INTRODUCTION. 2. CADRE THÉORIQUE. 2.1. Le capital intellectuel. 2.2. L'économie sociale et le corps de la Guardia Civil. 3. MÉTHODOLOGIE. 4. RÉSULTATS ET DISCUSSION. 5. CONCLUSIONS ET PROPOSITIONS. 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : Dans l'environnement socio-économique actuel, la sécurité est une question clé pour la coopération entre les pays qui composent l'Union européenne. Cela implique que les politiques du secteur public ne doivent pas seulement renforcer les capacités de défense, mais aussi mettre en œuvre des mesures qui contribuent à la sécurité économique et sociale. L'association de ces termes : sécurité, coopération, économie publique et sociale, nous amène à penser à une institution qui les a alignés dans sa stratégie depuis plus de 181 ans d'existence, l'Institution de la Garde Civile. Cependant, nous n'avons pas trouvé de recherches, d'articles ou de projets qui abordent cette question dans la sphère académique. Cette étude analyse comment le capital intellectuel (CI) de l'institution contribue à générer de la valeur socio-économique à travers ses actions solidaires et humanitaires. La méthodologie utilisée est basée sur une analyse de contenu des informations divulguées sur son CI dans ses rapports de responsabilité sociale et de durabilité entre 2014-2023. Le modèle Intellectus adapté au contexte public a été utilisé pour identifier et quantifier les actifs immatériels. Les résultats montrent que le CI de l'institution, grâce à la gestion des connaissances, à la culture organisationnelle, aux relations extérieures, au caractère bienveillant et à l'engagement social, apporte une valeur tangible et intangible qui va au-delà de ses fonctions de sécurité publique. Cette recherche démontre la pertinence du CI dans les institutions publiques et son potentiel dans le renforcement d'une économie sociale intégrée dans l'Agenda 2030.

Resumen: La seguridad es un tema clave para la cooperación entre los países que conforman la Unión Europea en el entorno socioeconómico actual. Esto implica que las políticas del sector público no sólo fortalezcan las capacidades en defensa, sino que también implementen medidas que contribuyan a la seguridad económica y social. Conectando estos términos: seguridad, cooperación, público y economía social, nos lleva a pensar en una institución que los ha alineado en su estrategia, durante más de 181 años de existencia, la Institución de la Guardia Civil. Sin embargo, no se han encontrado investigación, artículos o proyectos que aborden esta cuestión en el ámbito académico. El presente estudio analiza cómo el capital intelectual (CI) de la institución, contribuye a generar valor económico-social a través de sus acciones solidarias y humanitarias. La metodología utilizada se basa en un análisis de contenido de la información divulgada de su CI en sus memorias de responsabilidad social y de sostenibilidad entre 2014-2023. Se ha empleado el modelo Intellectus adaptado al contexto público, para identificar y cuantificar los activos intangibles. Los resultados evidencian que el CI de la Institución, a través de la gestión del conocimiento, la cultura organizativa, las relaciones externas, el carácter benemérito y el compromiso social aporta valor tangible e intangible que va más allá de sus funciones de seguridad pública. Esta investigación demuestra la relevancia del CI en instituciones públicas y su potencial en el fortalecimiento de una economía social integrada en la Agenda 2030.

Mots-clés : économie sociale, capital intellectuel, garde civile, durabilité, valeur sociale.

Palabras clave: economía social, capital intelectual, guardia civil, sostenibilidad, valor social.

ABBREVIATIONS

ASGC : Association des gardes civils solidaires.

CEPES : Confédération espagnole des entreprises de l'économie sociale.

CE : Capital structurel.

CH : Capital humain.

QI : capital intellectuel.

CIC : Centre de recherche sur la société de la connaissance.

CIS : Centre de recherche sociologique.

RC : Capital relationnel.

EUROPOL : Police européenne.

IADE : Institut d'administration des entreprises.

KBW : Knowledge- Based View (vision basée sur la connaissance).

MITES : Ministère du travail et de l'économie sociale.

MRSCGC : Rapport sur la responsabilité sociale des entreprises de la Guardia Civil.

MS : Rapport sur le développement durable.

RBV : Resources- Based View (vision basée sur les ressources).

RSE : Responsabilité sociale des entreprises.

SDGs : Sustainable Development Goals (objectifs de développement durable).

OECC : Office espagnol du changement climatique

OCDE : Organisation de coopération et de développement économiques.

ONG : Organisation non gouvernementale.

ONU : Nations unies.

OTAN : Organisation de l'Atlantique Nord.

UE : Union européenne.

VRIN : valeur, rareté, inimitabilité et non-substituabilité.

1. INTRODUCTION

L'économie sociale est un modèle économique axé sur l'intérêt collectif qui place les personnes au centre de son activité, en donnant la priorité à la coopération, à la durabilité et à la solidarité plutôt qu'au profit individuel (Retolaza & Alzola, 2021). Le développement continu des économies et des sociétés exige de donner la priorité aux mesures qui améliorent la productivité dans tous les secteurs industriels. Il est particulièrement intéressant d'analyser comment une institution publique telle que la Guardia Civil, qui place les personnes au centre de son modèle d'entreprise, intègre les principes de l'économie sociale dans sa mission de garantie de la sécurité publique.

Actuellement, l'économie sociale a été promue par le Comité économique et social européen, en mettant l'accent sur l'interdépendance entre l'économie et la société. En Espagne, le concept a été largement diffusé par la Confédération espagnole des entreprises de l'économie sociale (CEPES). En outre, la loi 5/2011, du 29 mars, dans son préambule, regroupe les principes de différenciation des entités de l'économie sociale, l'un d'entre eux étant l'accent mis sur les personnes et l'objectif social, en tant que principal. Dans ce contexte, les organisations participantes accueillent des projets sociaux réalisés individuellement, en tant qu'institutions ayant une autre forme juridique (Sánchez et al., 2018). Aligné sur le Plan global pour une culture de la sécurité nationale, car il est développé conformément aux Objectifs de développement durable (ODD) fixés par l'Agenda 2030. Pour évoluer, elle nécessite la collaboration active de tous les secteurs qui composent l'écosystème social, des organisations privées aux organisations publiques, en passant par les organisations de la société civile, sans oublier le secteur académique (García-Flores & Palma, 2020).

Dans le prolongement du point précédent, on pourrait dire que l'institution de la Garde civile appartenant au secteur public présente une approche intégrée dans l'économie sociale à travers les dimensions ou les capitaux qui composent son capital intellectuel (CI). Depuis sa création, l'institution de la Garde civile fonde ses actions sur la sécurité, la prévention et la protection des droits et libertés des citoyens, mais aussi sur leur prise en charge et leur assistance lorsqu'ils se trouvent dans une situation de vulnérabilité (capital humain). En ce sens, elle encourage la participation et la coordination interne et externe avec différentes entités, ce qui est connu comme un caractère bienveillant (capital structurel). Cet intangible, combiné à d'autres tangibles tels que la structure et la diversification de l'institution, sert non seulement à renforcer les alliances qui favorisent les réseaux sociaux déjà établis, mais il est également utilisé comme facilitateur de connexions entre des communautés et des individus éloignés (Burt, 2004) (capital relationnel). Sans oublier que la cohésion et la confiance générées par ces relations facilitent la transmission des connaissances, qui constituent un bien immatériel précieux dans l'économie (Arteaga et al., 2020).

La recherche sur le CI a montré la pertinence de la valeur qui lui est attachée. Garanina et al. (2021), dans une étude structurée menée dans différents pays au cours de la période (2010-2020), ont observé la convergence des chercheurs pour conceptualiser le concept de CI en tant que générateur de valeur commerciale. Dans le présent document, nous éviterons d'entrer dans la rhétorique sur la valeur des actifs incorporels par rapport aux actifs corporels, car aujourd'hui, la controverse de l'ère post-industrielle des années 1970 a été laissée de côté. La valeur des actifs incorporels d'une entreprise commençait alors à faire l'objet d'un débat dans le cadre de l'information financière. Les controverses

soulevées à leur sujet après l'éclatement de la bulle Internet, la crise financière mondiale de 2008, lorsque les entreprises ont commencé à évaluer les "risques", et une période de relative stagnation économique sont tout aussi oubliées (Hazan et al., 2021).

L'académie indique que le paradigme du CI est considéré comme établi comme un système pour la réalisation de la valeur de l'entreprise parmi les universitaires à la fin de 2010 et, par conséquent, a atteint la consolidation théorique dans nos jours. Par conséquent, l'objectif de cette étude est d'analyser dans quelle mesure les actions solidaires et humanitaires de l'institution de la Garde civile génèrent une valeur sociale pour les parties prenantes, en ayant un impact sur l'économie sociale à travers la gestion des éléments qui composent son CI, car ils sont la clé de la croissance et du développement social (Haskel & Weslake, 2018 ; Stratone, 2023). Notre décision repose sur le fait de combler une lacune constatée dans l'application d'une approche de CI à une institution publique en tant qu'agent actif de l'économie sociale et traditionnellement étudiée à travers un prisme opérationnel et juridique. En rendant ces principes visibles dans l'institution de la Garde civile, nous visons à ouvrir d'autres lignes de recherche qui n'ont pas été aussi explorées dans l'économie sociale et dans les organismes nationaux et internationaux d'application de la loi dans leur étude de la CI.

Cet article est structuré de la manière suivante : dans la première section, nous rappelons et définissons brièvement le concept de Capital Intellectuel (CI). Ensuite, dans la deuxième section, nous analysons les synergies entre l'économie sociale et l'institution qui fait l'objet de notre recherche et nous en déduisons nos hypothèses de recherche. Ces hypothèses sont exposées dans la troisième section, qui traite de la méthodologie utilisée. Dans le prolongement de cette dernière, la quatrième section présente les résultats obtenus par la recherche et se termine par la cinquième section sur les conclusions tirées, les contributions et les limites.

2. CADRE THÉORIQUE

2.1. LE CAPITAL INTELLECTUEL (CI)

Les entreprises de tous les secteurs, au niveau micro ou macro, doivent tenir compte de leurs actifs tangibles et intangibles utiles à la création de valeur, souvent appelée capital intellectuel (Cañibano et al., 2002 ; Bueno et al., 2008 ; Fernández et al., 2022). Cette notion prend de l'importance lorsque l'on établit l'importance des actifs incorporels dans l'économie des entreprises et que l'on positionne l'investissement dans les actifs incorporels par rapport aux actifs corporels. Des études montrent que les actifs incorporels sont essentiels à la croissance de l'économie et des entreprises (Haskel & Weslake, 2018 ; Stratone, 2023), notamment en raison de leur accélération après la pandémie de COVID-19 (Hazan, 2021). Cependant, cela n'a pas toujours été le cas, si nous passons en revue les études antérieures sur les actifs incorporels, nous trouvons au début des années 1990 la genèse du concept de CI.

Après l'ère post-industrielle des années 1970, les entreprises ont commencé à s'interroger sur les actifs incorporels. Quelques décennies plus tard, les économies mondialisées et en réseau des années 1990 ont démontré l'importance de l'actif immatériel que constituent les flux d'informations internes et externes, les connaissances accumulées et les procédures exclusives. Il s'agissait d'actifs incorporels qui n'apparaissaient pas dans les états financiers, mais qui contribuaient à la réalisation des objectifs de l'entreprise. On

peut donc dire que le CI est né de la volonté de connaître le produit résultant de la soustraction de la valeur réelle d'une entreprise et de sa valeur de marché.

Edvinsson et Malone (1999) tentent de l'expliquer par la métaphore selon laquelle le QI serait les racines d'un arbre, quelque chose que l'on ne voit pas, mais qui est nécessaire à la croissance. Pour ces auteurs, il se compose de l'infrastructure, des relations avec les partenaires et les clients, et des compétences des employés. D'autres auteurs, comme Johnson (1999), mettent l'accent, dans ce groupe d'intangibles, sur l'intelligence humaine et l'innovation en tant que générateurs de profit. Une revue de la littérature sur le QI nous amène à extraire les théories influentes comme piliers de son développement :

1. *La vision basée sur les ressources (RBV)*. Barney (1991) postule que, pour être compétitives, les ressources d'une entreprise doivent être précieuses, rares, inimitables et non substituables, popularisant ainsi dans le monde universitaire et dans la pratique les critères de la RBV. La stratégie d'entreprise se concentre sur les pratiques et les processus impliqués dans l'activité quotidienne développée dans l'organisation et ses résultats (Potter, 1996). Cette théorie commencera à conceptualiser non seulement les ressources tangibles, mais aussi les ressources intangibles telles que la connaissance (Grant, 1996).

2. *Théories de la vision basée sur la connaissance (KBW)*. Dans la nouvelle société de la connaissance, c'est la ressource par excellence. Sa principale exponentielle est la spirale de la connaissance, largement popularisée par ses créateurs Nonaka et Takeuchi (1995). Leur vision de l'entreprise est celle d'une entité active de création et de diffusion de connaissances. À cette fin, la connaissance tacite, celle qui est inarticulée, intuitive, découle de l'expérience de l'individu "dans" et "avec" le travail qu'il effectue "know how" (Nonaka & Takeuchi, 2021). Il est transmis et en même temps transformé dans l'organisation lorsqu'il est appliqué (Grant, 1996) en connaissances explicites. Elles peuvent être codifiées, écrites, objectives et facilement transférées (Nonaka & Konno, 1998), le "know about" étant créé au niveau de l'organisation et de l'individu. Cette théorie lui confère un dynamisme et une projection externe qui faisaient défaut à la théorie précédente (Bontis, 2002).

3. *La théorie des capacités dynamiques*. Comme l'ont indiqué ses précurseurs (Teece et al., 1997), elle se concentre sur la capacité combinatoire des entreprises à faire en sorte que leurs connaissances, leurs compétences et leur expérience restent intégrées dans leurs produits et leurs processus et soient difficiles à imiter. Bien que plus moderne que celles évoquées ci-dessus, elle s'est étendue aux domaines suivants : l'entrepreneuriat (Alvarez & Barney, 2001) ; la performance des entreprises (Wang et al., 2011 ; Stratone, 2023) ; le retour sur investissement (Chen et al., 2009 ; Tan et al., 2007) ; les environnements en réseau (Zheng et al., 2011) et l'environnement (Chen, 2008 ; Haarhaus & Liening, 2020).

Ces théories conduisent à définir le CI comme l'ensemble des ressources matérielles et immatérielles et la capacité des entreprises à les gérer, ce qui les rend compétitives et durables.

2.1.1 Définition et dimensions du QI

L'analyse de la littérature n'a pas permis de trouver une définition universellement

acceptée du CI. Malgré cela, les auteurs s'accordent à montrer comment son identification et son utilisation créent des avantages pour l'organisation (Hazan et al., 2021 ; Sumedrea, 2013). Les contributions de certains auteurs pertinents qui ont étudié le CI sont présentées ci-dessous (tableau 1).

Tableau 1
Principales contributions aux définitions de l'IC.

Aportaciones a la definición del CI	Autor
Sistemas y procesos que la hacen competitiva.	Steward, 1997
Los activos que no están en los estados financieros pero deberían reflejarse.	Petty & Guthrie, 2000; Roos, 2001 Reed et al. 2006; HernandezBueno et al., 2008
Fuente de futuros beneficios.	Lev, 2001
Necesarios para la innovación.	López et al., 2004; Rideg et al., 2023
Impulsor de la innovación y factor clave en la economía.	OECD, 2006
Combinación de intangibles y tangibles alineados a la estrategia empresarial para generar beneficios.	Bueno et al., 2008
Conocimiento a disposición de la organización para decidir las estrategias.	Aramburu et al, 2015
Creación de valor	Cañibano et al., 2002 Demartinni &Trucco, 2016 Garanina et al., 2021
Motor del desarrollo económico y social	Merino et al., 2018 Suciu & Năsulea, 2018
Creación valor corporativo y generación ventajas sostenibles en economías emergentes	Xu & Wang, 2018
Recursos estratégicos.	García-Flores & Palma., 2020
Motor de la cuarta revolución industrial.	Li et al., 2020
La tecnología es impulsora de las relaciones sociales que posibilitan su difusión.	Briñez, 2021
Rápido crecimiento económico.	Hazan et al., 2021
Efectos en el valor del mercado	Dumay et al., 2016
Mejora el desempeño organizacional	Thum-Thysen et al., 2021 Fernández-Solís et al., 2025

Dans cette étude, nous définissons le CI comme des valeurs immatérielles qui, lorsqu'elles sont gérées conjointement avec des valeurs matérielles, contribuent à la croissance commerciale, économique et sociale.

Tout comme il n'existe pas de consensus sur la définition du QI, il n'y a pas de modèle universellement accepté pour sa mesure. Au fil du temps, divers modèles ont tenté de classer la mesure des actifs incorporels, évoluant de modèles plus simples tels que Skandia (1997) à des modèles plus complexes tels que le modèle Intellectus mis à jour (2011).

Parmi les pionniers de la mesure du QI, le Skandia Navigator d'Edvisson et Malone (1997) regroupe les éléments qui composent le QI en deux dimensions pour son étude : le capital humain et le capital structurel. En revanche, la plupart des auteurs qui se consacrent à l'étude du CI s'accordent à regrouper les intangibles qui le composent en trois capitaux : le capital humain (HC), le capital relationnel (RC) et le capital structurel (SC) (Petty & Guthrie, 2000 ; Navarro & Medina, 2024). Pour illustrer cela, nous présentons les classifications en capitaux avec leurs éléments dans le tableau 2. La première colonne présente les indicateurs de Johnson (1999), qui a apporté à la littérature

Capitales	Elementos no financieros	Elementos CE y OCDE
Capital Humano (CH)	Habilidades; conocimientos; tareas y motivación	Capacidades, saberes, habilidades y experiencias
Capital Estructural (CE)	Procesos de negocio y renovación, flow de información, productos y servicios; formas de cooperación de procesos	Procedimientos, rutinas organizativas, cultura, sistemas, bases de datos, licencias, etcétera.
Capital Relacional (CR)	Relaciones con los socios, clientes, proveedores e inversores	Relaciones con clientes, proveedores, socios de I+D+i.

une distinction claire entre les indicateurs financiers et non financiers en relation avec la valeur de marché d'une entreprise. La deuxième colonne montre la classification réalisée par Cañibano et al. (2002) sur la base du projet MERITUM¹ promu par l'OCDE et la CE ; elle a été représentée parce que l'institution s'inscrit dans ce contexte.

Tableau 2
Exemples de catégories de CI et de classifications d'indicateurs.

Pour ces auteurs, le CI est la combinaison des éléments qui composent les capitaux dont disposent les entreprises. Cependant, dans la revue de littérature, nous avons également trouvé des auteurs tels que Delgado et al. (2008), qui préfèrent l'étudier en le divisant en cinq dimensions : le capital humain, le capital technologique, le capital organisationnel, le capital relationnel et le capital social. En suivant cette dernière catégorisation du CI, on pourrait donc s'interroger sur la pertinence d'extraire le capital social du CI et de l'aligner sur l'économie sociale. L'objection que nous soulevons est que le capital social, que ce soit en tant que dimension ou en tant que subdivision du capital relationnel, ne crée pas de valeur en soi sans l'interaction des deux autres capitaux, comme nous l'expliquons ci-dessous.

¹ Mesurer l'immatériel pour comprendre et améliorer la gestion de l'innovation (MERITUM) : projet conjoint OCDE-CE visant à stimuler la recherche en Europe (1998-2001).

À cette fin, nous définissons ici, sous une forme synthétisée, les dimensions dans lesquelles les éléments qui composent le QI sont généralement classés par les universitaires en vue de leur étude, ainsi que la manière dont ils sont liés :

- La dimension du capital humain (CH) comprend les connaissances établies chez les employés d'une entreprise ; les individus sont capables de les générer (Delgado et al. 2008). Il réside dans les capacités, les compétences, l'expérience (Bueno & Merino, 2007 ; Bellucci et al., 2021), les valeurs et les attitudes à l'égard de l'entreprise et de l'emploi. En outre, ce capital inclut celui des salariés, qui sont des sources actives de connaissances utiles pour l'organisation (Merino et al., 2018). La relation avec les deux autres capitaux se manifeste à la fois dans l'innovation (Li et al., 2020), car ce sont les individus d'une organisation qui demandent de nouvelles façons de faire les choses (CE) et dans la capacité à travailler avec les autres et à négocier, ce qui nécessite motivation, loyauté et satisfaction (CE, 2006) (CR).

- Pour la plupart des auteurs (Chen et al., 2009 ; Delgado et al., 2008 ; Dumay et al., 2016 ; Merino et al., 2018, Oliveira et al., 2020), la dimension du capital structurel (CS) est constituée d'actifs tels que : la structure organisationnelle, les routines, les procédures, les processus, les bases de données, les manuels, les brevets et les logiciels, qui restent dans l'entreprise lorsque les personnes qui y travaillent ont terminé leur travail. Certains de ces actifs sont tangibles, comme les machines et la structure. D'autres sont intangibles, comme la propriété intellectuelle, les marques, les brevets, la culture organisationnelle (Chen et al., 2009) et l'image (Merino et al., 2018 ; Jeffrey et al., 2019). La relation la plus notable avec les deux autres capitaux repose sur la structure de l'organisation. Celle-ci sert d'échafaudage par lequel les processus et les procédures sont transférés entre le capital humain et le capital technologique, créant ainsi des relations entre les *parties prenantes*.²

- La dimension du capital relationnel (RC) couvre les actifs générés par l'ensemble des relations entre les employés, les clients, les fournisseurs, les actionnaires (Bellucci et al., 2021), les alliances stratégiques qui génèrent des informations et des connaissances pertinentes pour l'entreprise. La synergie générée avec les autres capitaux peut être illustrée par les relations formelles et informelles entre les employés de l'organisation, car elles sont essentielles à la transmission et à la génération d'informations et de connaissances (CH). En ce qui concerne le CE, nous constatons que ces connaissances sont diffusées d'un individu à l'autre et sont également transformées en restant dans les organisations (De Castro & García, 2003), influençant ainsi l'économie et la société (Garanina et al., 2021). L'importance de ce capital relationnel est perçue dans la segmentation des clients que les entreprises effectuent habituellement, dans la création ou la diminution des accords commerciaux et dans l'établissement ou le renforcement des alliances, car tout le monde n'a pas les mêmes besoins ou ceux-ci changent au fil du temps.

² Les *parties prenantes*. Pour le pionnier Friedman, les *parties prenantes* sont toutes les personnes qui influencent ou sont influencées par une entreprise. Les parties prenantes de la Guardia Civil comprennent les citoyens, les administrations publiques, les gardes civils et d'autres organisations telles que les ONG, la sécurité privée, les universités et les forces de police internationales. Parmi ces parties prenantes, on trouve également des personnes aux intérêts opposés qui appartiennent à des gangs criminels, des groupes terroristes, des criminels, etc.

Ainsi, c'est l'interaction des capitaux susmentionnés qui crée de la valeur dans une organisation. Nous l'illustrons par la production de connaissances, reconnue comme un élément clé du développement économique (OCDE, 2006). Les informations et les connaissances sont diffusées par des structures humaines ou technologiques (Devenpor & Prusak, 2001 ; Wang, 2011) ou les deux (CH). Nous savons également qu'elles sont accumulées dans ces structures par le biais de processus, d'opérations, de routines organisationnelles, de procédures, etc. (De Castro & García, 2003), qui constituent l'échafaudage des activités commerciales et sociales et permettent de créer de la valeur organisationnelle (Demartinni & Trucco, 2016) (EC). Dans une mesure plus ou moins grande, le développement d'un réseau est encouragé, en favorisant les schémas de participation, la collaboration, le développement d'initiatives et de plates-formes sociales (CR). Cependant, ce réseau, même dans son état optimal, pourrait entraver le flux de connaissances, en raison des éléments qui le composent, tels que : avoir un personnel insuffisant ou mauvais, une mauvaise gestion, ou même que les procédures ou les politiques de la stratégie de l'entreprise interfèrent négativement dans ce réseau (Merino et al., 2018).

En guise de conclusion théorique, il ne fait aucun doute que le fait de se concentrer sur la valeur réelle d'une entreprise et de la déterminer a été le *moteur du* développement du capital intellectuel. L'objectif était d'expliquer le résultat de la différence constatée entre la valeur d'une entreprise dans ses livres financiers et sa valeur de marché. Cette valeur, expliquée au CI, est due à l'interaction des éléments qui la constituent tels que : les compétences, les connaissances et l'expérience des employés ainsi que les projets de R&D&I ; les routines organisationnelles ; l'interaction des relations internes et externes (Briñez, 2021) tant au niveau des employés qu'avec les fournisseurs, les actionnaires, les alliés et les clients (CE, 2006)³. Sans oublier la gestion de la transformation, de l'acquisition et de l'application dans un environnement changeant (Nonaka & Takeuchi, 2021).

Ces caractéristiques positionnent le CI comme une clé de la croissance économique (Bellucci et al., 2021), sociale et durable (Secundo et al., 2020) adaptée à un marché volatile, diffus, incertain, ambigu, complexe (Nonaka & Takeuchi, 2021) et technologiquement perturbateur (Wang et al., 2021). C'est pourquoi, dans la section suivante, nous expliquerons empiriquement, à travers l'institution de la Garde civile, comment les entreprises peuvent fournir des avantages socio-économiques par le biais du CI.

2.2. L'ÉCONOMIE SOCIALE ET LE CORPS INSTITUTIONNEL DE LA GARDE CIVILE

L'économie sociale⁴ est définie comme un ensemble d'activités commerciales et économiques menées par des entités en vue de la réalisation du bien collectif de ses membres, de l'intérêt économique et/ou social général selon les principes de l'économie sociale (MITES, 2025). Actuellement, le concept est consolidé en Espagne et diffusé par le Centre international de recherche et d'information sur l'économie publique, sociale et

³Document RICARDIS de l'UE (2006). La Commission européenne s'appuie sur cette interaction basée sur le projet MERITUM, 2002. Il est défini comme la combinaison du capital humain, du capital structurel et du capital relationnel, des ressources et des activités d'une organisation.

⁴ Il est actuellement promu par le Comité économique et social européen et se concentre sur l'interdépendance entre l'économie et la société.

coopérative. Si nous mettons en relation ces termes : public, social, coopératif et économie publique, cela nous amène à penser à une organisation qui les a alignés dans sa stratégie pendant plus de 181 ans d'existence : l'institution de la Garde civile, en faisant converger les pratiques économiques et sociales dans la fourniture de biens et de services. Nous nous appuyons sur la découverte, au sein de l'institution, de principes établis de l'économie sociale et collaborative tels que ceux énumérés ci-dessous, par des auteurs tels que Díaz-Foncea et al :

- Promouvoir la solidarité entre les employés en facilitant les structures, en les motivant à faire preuve de solidarité et de coopération.
- Reconnaissance de la solidarité et de l'engagement à travers l'esprit du mérite.
- Promotion de l'égalité au sens large, pas seulement sur la base du sexe.
- Inclusion et cohésion sociale.
- Aider et soutenir les groupes les plus vulnérables et ceux qui sont menacés d'exclusion sociale.
- Conciliation de la vie professionnelle et de la vie familiale.
- Générer la durabilité en interne et en externe, dans le respect de

Diferentes Cuerpos de Seguridad Artículo 11 (página 26)	Específicos de la Guardia Civil Artículo 12, B (página 27)
• Velar por el cumplimiento de las leyes y disposiciones generales. • Auxiliar y proteger a personas y bienes. • Vigilar y proteger edificios públicos. • Mantener el orden y velar seguridad ciudadana. • Prevenir la comisión de actos delictivos. • Investigar delitos, asegurar las pruebas e instrumentos poniéndolos a disposición del juez. • Prevención de la delincuencia. • Colaborar con Protección Civil, caso grave de riesgos o catástrofes.	• Control de armas y explosivos. • Resguardo Fiscal del Estado (costas, fronteras, puertos y aeropuertos) • Vigilancia del tráfico, tránsito y transporte en las vías públicas interurbanas (exceptuando el País Vasco y Cataluña). • Conservación de la naturaleza y medioambiente, recursos hidráulicos, riqueza forestal y de otra índole relacionada con la naturaleza. • Conducción interurbana de presos y detenidos. • Aquellas otras que les atribuye la legislación vigente.

l'environnement et de la protection de la biodiversité.

L'avantage concurrentiel de cette institution est d'offrir des services de qualité supérieure afin d'être une référence dans son secteur, devant les citoyens, l'État et l'Union européenne. Sa mission, au sein des forces et corps de sécurité de l'État, est de "*protéger le libre exercice des droits et libertés et de garantir la sécurité publique*" (art. 104 de la Constitution). Elle le fait en plaçant les personnes au centre de son action, en assurant leur sécurité et leur intégrité, dans la proximité. Les fonctions sont présentées dans le tableau 3.

Tableau 3

Définition des compétences fonctionnelles de la Garde civile

Note : Les données de ce tableau sont basées sur la loi organique 8/1986 du 13 mars 1986 et sur les rapports de durabilité de la Guardia Civil, 2023.

En plus des fonctions présentées dans le tableau ci-dessus, en partageant des compétences avec d'autres forces de police régionales et nationales, la Guardia Civil est responsable de la sécurité des citoyens sur 84,53% du territoire national et de la mer territoriale (CG, 2023). D'autre part, en tant que force de sécurité publique de nature militaire, elle peut mener des missions internationales en rejoignant une organisation internationale telle qu'EUROPOL, l'ONU ou l'OTAN, ainsi que les forces armées espagnoles (CG, 2023).

On peut dire qu'avec plus de 80 000 hommes, elle est déployée sur l'ensemble du territoire national et international. Elle est diversifiée en spécialités : Protection de la nature, Police judiciaire, Services d'information et Service maritime, entre autres. À cela s'ajoute le potentiel humain déployé dans la sécurité des citoyens, avec plus de 2 000 unités territoriales (CG, 2025).

2.2.1 Valeur sociale créée par l'institution.

La valeur sociale peut être définie comme le résultat positif des actions développées par une entité sur la société (Retolaza & Alzola, 2021). Cette valeur immatérielle est contextualisée dans l'engagement des gardes civils à aller au-delà de l'accomplissement de leur mission. Ils le font en tant que contribution sociale, en se concentrant à la fois sur l'amélioration de la vie et le soutien des citoyens, ainsi qu'en étant conscients des préoccupations environnementales, conformément à l'un des principes de l'économie sociale énoncés par Díaz et Lejarriaga (2019). Par exemple, en ce qui concerne ce dernier principe, elle a enregistré son empreinte carbone auprès de l'Office espagnol du changement climatique (OECC), devenant ainsi l'une des seules forces de police à le faire au niveau mondial. Nous soulignons également le prix décerné par les Nations unies en 2023, "Prix de la protection de l'ozone pour les agents des douanes et de la police".

Ces valeurs sont renforcées par l'institution grâce à la transparence et à la reconnaissance de ses actions, en présentant un impact intégrateur et collaboratif, où les communautés au sein desquelles ses projets sont développés ont un rôle dans la prise de décision, sur ce qu'elles considèrent comme une valeur. Par conséquent, l'institution combine ses ressources, ses politiques et ses processus pour améliorer la vie des personnes et de la société en général, ce que l'on appelle la valeur sociale (Retolaza & Alzola, 2021).

Pour développer ses capacités, son modèle d'entreprise consiste à diffuser et à appliquer une culture de la sécurité de qualité, polyvalente, disponible et proche du citoyen. Pour ce faire, elle transmet ses connaissances et son expérience à d'autres forces de police nationales et internationales, aux citoyens, au gouvernement et à d'autres parties prenantes, avec professionnalisme et bienveillance. Ce dernier est reconnu parce que les gardes civils travaillent avec la connaissance et l'engagement de faire des choses extraordinaires, contribuant à ce que nous avons appelé les intangibles.

Il convient de rappeler que dans le premier règlement de service de 1844, l'article 32 indiquait déjà sa nature charitable et protectrice. À la même époque, l'article 6 de la Charte de la Guardia Civil stipulait que la Guardia Civil devait prendre soin des personnes non protégées et être un heureux pronostic pour les personnes affligées (GC, 2025). Quelques années plus tard, en 1929, l'institution s'est vu décerner la Grand-Croix de l'Ordre civil de la Charité avec un insigne noir et blanc, qui implique un risque personnel,

en reconnaissance des services humanitaires et héroïques qu'elle a rendus. On peut donc dire que la solidarité et la coopération sont des valeurs inscrites dans l'ADN de l'institution depuis sa création, devenant ainsi la marque de l'identité de l'Institut.

L'esprit, ou le caractère bienveillant, est encore présent aujourd'hui, exprimé dans son code de conduite⁵. L'article 21 prévoit la fourniture d'une assistance aux citoyens, que le personnel soit en service ou non. On le retrouve également dans le point 7 du décalogue des membres de la Guardia Civil, qui stipule qu'ils doivent toujours aider ceux qui en ont le plus besoin, en se concentrant sur les personnes en situation de vulnérabilité et de manque de protection ; il est également exprimé dans leurs rapports de responsabilité sociale d'entreprise (MRSC) et dans le magazine officiel de la Guardia Civil.

C'est pourquoi l'institution promeut ce bien immatériel, qu'elle considère comme un actif organisationnel, en le promouvant par le biais de services humanitaires, du volontariat, de la lutte pour la biodiversité et l'environnement. Il est produit, tant au niveau individuel que dans d'autres organisations, comme indiqué sur son site web #GComprometidos.

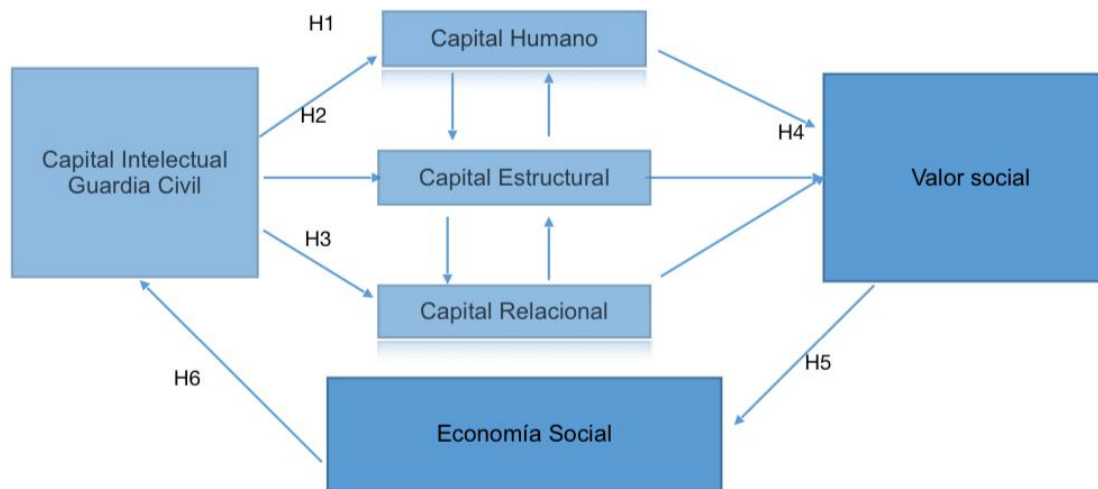
Compte tenu de ce qui précède, nous pouvons dire que la mission de la Garde civile n'est pas seulement basée sur la sécurité publique, mais qu'elle inclut également le bien-être de la société, qui est déterminé par le dynamisme fourni par les dimensions de la CI qui la composent, générant une croissance économique (Nonaka & Takeuchi, 2021). Cependant, cette valeur économique-sociale n'est pas prise en compte ou est inconnue dans le monde académique, puisque, lorsque nous avons mené notre recherche, nous n'avons pas trouvé d'études, de recherches ou d'articles sur le sujet. C'est pourquoi, dans la section suivante, nous exposerons nos hypothèses sur la contribution de la valeur économique sociale de l'institution dans le modèle de recherche.

3) MÉTHODOLOGIE

Sur la base de ce qui précède, nous présentons le modèle de recherche (figure 1) dans lequel les hypothèses de cette étude sont énoncées :

⁵ Décret royal 176/2022 du 4 mars, approuvant le code de conduite de la Garde civile.

Figure 1.
Modèle de recherche et hypothèses.



H1. Le capital humain est identifié dans l'institution.

H2. Le capital structurel est identifié dans l'institution.

H3. Le capital relationnel est identifié dans l'institution.

H4. L'interrelation des trois capitaux a un impact sur la création de valeur sociale.

H5. La valeur sociale générée influence l'économie sociale.

H6. L'économie sociale influence le capital intellectuel de la Guardia Civil.

Afin de tester nos hypothèses, nous avons suivi les indications de Codina et al. (2020) en réalisant une revue de littérature à l'aide de bases de données scientifiques telles que SCOPUS, Web of Science et Google Scholar. Ces auteurs montrent dans leur recherche que ces bases de données, utilisées par la communauté scientifique internationale, couvrent largement tous les domaines de la connaissance. La recherche a été effectuée à la fois dans les champs : titres d'articles, dans le *résumé* ou par les mots-clés indiqués dans cet article. Cependant, la recherche n'a donné aucun résultat, démontrant le manque d'articles scientifiques sur notre sujet de recherche. Pour cette raison, nos données ont été obtenues à partir de la revue documentaire et bibliographique des bases de données du Ministère de l'Intérieur, ainsi que du Ministère de la Défense et de l'Institution de la Garde Civile, où l'Institution publie ses rapports financiers et non financiers. Nous nous appuyons donc sur des données quantitatives et qualitatives provenant de sources primaires ouvertes.

La technique choisie a été l'analyse de contenu⁶, car elle a été fréquemment utilisée avec succès dans l'analyse des rapports de divulgation sur le CI (Magau 2021 ; Dumay et al., 2016). Elle est également adaptée à la vérification d'hypothèses formulées de manière déductive (Bini & Giunta, 2017). Les corpus de l'analyse de contenu sont les rapports de responsabilité sociale de la Garde civile (MRSCGC) et les rapports de durabilité (MS). Notre décision est basée sur le fait que les rapports annuels sont des outils utilisés par les organisations pour communiquer à toutes les parties prenantes ce qu'elles considèrent comme important, en les divulguant (Petty & Guthrie, 2000 ; Bontis 2002 ; Guthrie & Abeysekera, 2006 ; Dumay et al., 2016). Conformément à la tendance actuelle, les entreprises divulguent leurs états financiers et non financiers aux parties prenantes dans ces rapports annuels (Dumay et al., 2016).

Il s'agit d'une étude longitudinale couvrant la période de 2014 à 2023, date des derniers rapports d'information annuels publiés. En plus de déterminer la cohérence des données, nous sommes en mesure d'obtenir la tendance institutionnelle en les analysant. Nous entendons répondre à la question de savoir si la contribution de l'institution à l'économie sociale lui est inhérente, conformément à l'objectif de notre étude.

L'unité d'analyse dans l'analyse de contenu est celle qui indique la présence ou l'absence des éléments à investiguer (Moreiro et al., 2006). Pour obtenir cette unité d'analyse, parmi les cadres conceptuels utilisés pour définir, classer et enregistrer les informations divulguées sur les CI, certains auteurs utilisent habituellement le modèle de Sveiby (1997) modifié par Petty et Guthrie (2000). Cependant, dans cette recherche, afin d'obtenir notre unité d'analyse, nous avons adapté les indicateurs du modèle Intellectus⁷ (2011) à l'institution, en raison de sa large répercussion nationale et internationale et parce qu'il est considéré comme un modèle intégratif pour mesurer le QI (Merino et al., 2018). Les considérations les plus notables de ce modèle sont les suivantes :

- La création d'un "arbre de pertinence" établissant une structure du CI, afin d'identifier les unités de mesure qui le composent, en établissant une hiérarchie de composants, d'éléments, de variables et d'indicateurs. Sur cette base, les catégories, les éléments, leurs définitions et les indicateurs ont été adaptés pour l'identification du CI dans l'institution (voir annexe I : tableaux 4 à 6).
- L'élaboration d'un indice synthétique, basé sur les principales composantes pour le quantifier. Celles-ci sont représentées dans une "carte des variables et des principaux indicateurs" qui sera utilisée comme mesure quantitative de l'ensemble des biens incorporels identifiables. À la suite de ce point, nous indiquons à l'annexe II les formules utilisées pour obtenir les indices.
- la préparation du rapport sur le contrôle interne (RCI) en vue de sa diffusion. Par conséquent, à la suite de la littérature, un examen des documents dans lesquels l'institution publie ses rapports financiers et non financiers a été effectué.

⁶ Pour Allport (1965), il s'agit d'une méthode d'étude et d'analyse des communications de manière systématique, objective et quantitative dans le but de mesurer des variables.

⁷ Document Intellectus, n°5 (2003) : il a été développé par le professeur Bueno et le Centre de recherche sur la société de la connaissance (CIC). Il a été modifié en 2011, donnant lieu au modèle Intellectus : Mesure et gestion du capital intellectuel, par l'IADE (Institut d'administration des entreprises). Les indicateurs adaptés sont tirés de son point 6. Tableau des indicateurs (pp. 36-58).

Nous avons réussi à limiter la subjectivité qui pourrait survenir lors de l'obtention de l'unité d'échantillonnage ou de l'unité d'analyse, en ajoutant de la transparence dans la catégorisation et en utilisant des règles de décision cohérentes tout au long de notre étude longitudinale. En ce qui concerne la fiabilité, l'instrument de codage a été manuel, sans recours à un logiciel, ce qui a permis d'éviter les problèmes posés par les mots à sens multiples qui, bien qu'ils puissent être réduits en augmentant les mots clés dans le contexte, ne détectent pas le sens du CI spécifique de l'institution, ni l'interprétation qui en est faite (voir annexe III : Phases de l'analyse de contenu).

Ensuite, afin de comprendre le comportement des variables de notre étude (dimensions du QI), nous les avons classées selon la division tripartite du QI : capital humain, capital relationnel et capital organisationnel. Nous nous basons sur celle-ci telle qu'elle a été établie par la Commission européenne (2006), sur la base du projet MERITUM (Cañibano et al., 2002) cité dans la section 2.2 (voir annexe I : tableaux 4-6).

Enfin, une analyse statistique des mesures de distribution de fréquence, de tendances et de dispersion a été réalisée. L'étude statistique vise à observer l'importance des éléments pour l'institution ainsi que leur comparaison et leur position par rapport aux autres éléments du CI, tout au long de la période étudiée. Pour ce faire, le programme statistique RStudio, version 2024.12.0+467 pour macOS 13+ a été utilisé.

4. RÉSULTATS ET DISCUSSION

Les résultats de notre recherche identifient le QI dans l'institution. Dans l'analyse de notre recherche, en adaptant le modèle Intellectus, les catégories, les éléments et les indicateurs, l'identification de ses éléments constitutifs est dérivée de la construction des catégories, des éléments et des indicateurs. Le CI de l'institution peut être classé en regroupant ses éléments constitutifs en capital humain, capital structurel et capital relationnel (voir annexe I). Ces résultats sont similaires à ceux de la plupart des études universitaires. Par conséquent, nous acceptons les trois premières hypothèses de cette recherche :

H1. Le capital humain est identifié dans l'institution.

H2. Le capital structurel est identifié dans l'institution.

H3. Le capital relationnel est identifié dans l'institution.

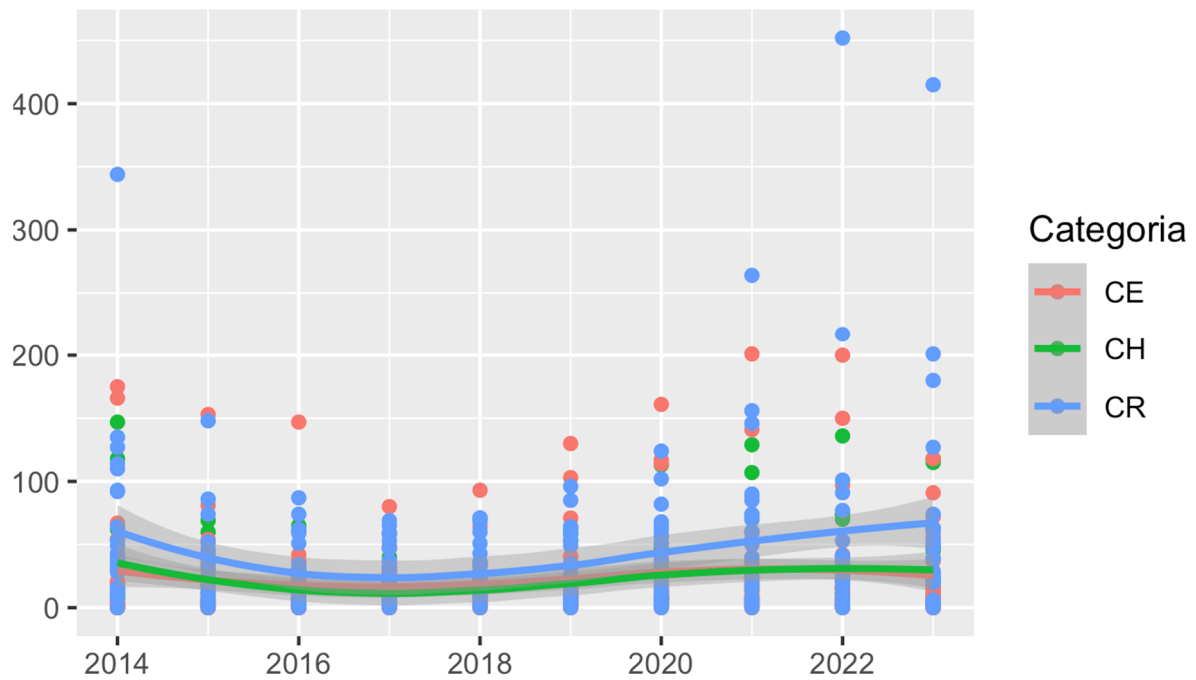
Nous procédons ensuite à la vérification des hypothèses restantes. En ce qui concerne la valeur sociale, en analysant le sujet des éléments qui composent les capitaux du CI et les capitaux de l'institution (annexe I), nous constatons que les définitions des éléments qui composent le capital humain, relationnel et structurel ont un impact direct sur la valeur sociale. En d'autres termes, les éléments du CI sont alignés sur l'identification de la valeur sociale dans la littérature, comme le montre le tableau 7 ci-dessous.

Tableau 7
Relation entre le QI de l'institution et la valeur sociale.

Dimensión Capital Humano			
Elementos	Definiciones	Capital Humano	Valor social
IDENTIDAD MOTIVACIÓN CREATIVO EDUCACIÓN ESPECIALIDAD; UNIVERSITARIO FORMACIÓN EXPERIENCIA DESARROLLO APRENDIZAJE CIVIL CONCILIA LIDERAZGO	Valores, motivación a la excelencia en sus actuaciones, formación especializada y conocimientos. Adaptación y generación ideas novedosas aplicables en el desarrollo del trabajo.	Autores como Nonaka y Takeuchi (2021) puntualiza que las empresas que cuentan con empleados con muchas habilidades y experiencia son capaces de gestionar escenarios cambiantes. Capacidad sin actitud o aptitud generaría una desaceleración o destrucción del valor (Merino et al., 2018)	Valor aportado por las personas a las empresas (Carina et al., 2024). Las creencias personales sobre un propósito social (Díaz-Foncela et al., 2016).
Dimensión Capital Estructural			
Elementos	Definiciones	Capital Estructural	Valor social
CULTURA CLIMA IGUALDAD ESTRUCTURA DESARROLLO RUTINAS RELACIONINT CRIMINAL PROVEEDORES INVERSIONIDI PERSONALIDI INFRAESTRUCTURA EQUIPOPOLICIAL INNGEST COMUNICACIONGC MARCA LICENCIAS SECRETO PATENTES TECNOEXT TECNOEW TECLIC PLEXIBILIDAD TALENTOS	Cultura institucional, idiosincrásica de la institución. Espíritu benemérito transferido generación a generación a través de acciones solidarias de cooperación, sacrificio y apoyo al necesitado. Seguridad y protección según la legislación vigente. La estructura de la Institución la hace distintiva, por su diversificación tanto geográfica como en especialidades para llegar a todos los ciudadanos. Andamiaje a través del cual el conocimiento, la experiencia y la información se transfiere diversificándose en especialidades aumentando así su valor empresarial. Sin olvidar las políticas e inversión en innovación y desarrollo.	Las empresas deben desarrollar su capital humano con los medios necesarios que apoye la visión sobre lo que las personas son capaces de hacer para generar cambio (Mohdzaini, 2021).	Recursos que los individuos pueden conseguir a través de la estructura de una organización (Sánchez et al., 2018). Sin estructuras sociales es difícil generar el capital social (Nonaka & Takeuchi, 2021).
Dimensión Capital Relacional			
Elementos	Definiciones	Capital Humano	Valor social
CIU LEALCIU QUEJAS PROTCIU ESTADO IADMINISTRACIÓN CAPITALEXTERIOR ALIANZAS ALIANZASESTABLES ALIANZASBENEFICIO CONCOMPETENCIA PRIVADA CERTICAL REDES ADMINISTRACIÓN MEDIOS DEFENSAMBIENTE VERDE MERCADO CODIGOCON ACSOCIAL BUENGGOBIERNO	Genera valor a través de las relaciones y alianzas establecidas con todos sus grupos de interés. En el plano internacional, establece relación de cooperación y colaboración con otros países. Es reseñable el apoyo a los más vulnerable y desfavorecidos. La inclusión y la cohesión social. Impulsa proyectos de voluntariado dentro y fuera de la institución. Dedicada a la defensa del medioambiente interna y externamente y la biodiversidad. Cuenta para ello con una red de medios de comunicación internos y externos promoviendo la transparencia y el buen gobierno.	Las empresas generan valor a través de las relaciones creadas con sus grupos de interés (Maqbool,2020) y en la transmisión de ese conocimiento (Rideg et al. 2023; Nonaka & Takeuchi, 2021). Este conocimiento debe ser fluido (Merino et al., 2018).	A través de promover el empleo, la inclusión social, sostenibilidad, innovación y crecimiento económico se consigue impulsar la economía social (cepes, 2023). Las empresas logran sus objetivos sociales promoviendo la transparencia (Sumedrea, 2013). Los programas de inclusión económica tienen un fuerte impacto en las personas más pobres del mundo (Word Bank, 2024).

Une fois les données quantifiées (annexe II) pour connaître le comportement des éléments de nos variables et savoir s'ils sont constants sur la période étudiée, une analyse de la distribution de fréquence et des mesures de tendance a été réalisée (figure 2).

Figure 2
Distribution de fréquence et tendances des éléments IC (2014-2023)



La figure 2 montre comment les éléments sont représentés au cours de la période étudiée et leur répartition en catégories. Il convient de noter que, si les courbes de dispersion du capital humain (HC) et du capital structurel (SC) sont presque alignées sur les dix années, indiquant la constance entre les fréquences des éléments des deux capitaux, celle du capital relationnel (RC) reste au-dessus d'eux. En outre, les scores aberrants des éléments de ce dernier capital sont les plus éloignés par rapport aux deux autres capitaux au cours des dernières années, ce qui montre la pertinence de ces éléments.

Ensuite, pour déterminer le regroupement de ces éléments, dans la figure 3, des mesures de tendance centrale et de position ont été utilisées. Un diagramme en boîte a été établi pour visualiser à la fois les mesures de position centrale (moyenne, médiane et mode) et les mesures de position non centrale, les quartiles, sur la base de notre connaissance de la dispersion des données de la figure 2.

Le tableau 8 montre la pertinence des éléments ayant obtenu les scores les plus élevés : Partenariats stables, Partenariats bénéfiques, Protciu, Social, Vert, Défesaenvironnement, au sein du CR. Les éléments : Criminel, Communications, Egalité, au sein de la CE et les éléments : Formation, Développement, Université et Créativité, au sein de la CH. Des scores élevés pour les éléments : Protciu et Asocial depuis 7 ans, Criminel depuis 8 ans et Communication depuis 10 ans.

Avec ces données (tableau 8) et les unités d'échantillonnage (annexe I), on peut déduire que pour l'institution, ses actions visent la sécurité, la protection des citoyens et le développement d'actions sociales par la force des partenariats et des services communs avec d'autres identités. Dans le même ordre d'idées, ses actions visent à protéger l'environnement et la biodiversité. Pour elle, la "valeur" n'est pas seulement considérée en termes financiers mais, à l'instar de Nonaka et Takeuchi (2021), "le social et l'environnemental" sont également des actifs précieux, constants en cela. À cette fin, son capital humain est égalitaire et diversifié, qualifié et développé, s'adaptant et créant de nouvelles idées dans l'exécution du service en transférant ses connaissances.

Ces résultats montrent que la définition de la valeur sociale suit celle de la valeur sociale en tant que résultat généré par la combinaison de ressources, de processus et de politiques qui améliorent la vie des personnes et la société dans son ensemble (Sánchez et al., 2018). Par conséquent, nous constatons que l'hypothèse 4 est corroborée :

H4 : L'interaction de ces capitaux génère de la valeur sociale.

En suivant notre ligne de recherche, nous allons maintenant découvrir comment cette valeur sociale a un impact sur l'économie sociale, au-delà de sa mission principale telle que décrite dans la section 2 : Protection et action sociale en faveur du citoyen (tableau 9), en suivant les principes de l'économie sociale et la définition de la valeur sociale.

Tableau 9
Indicateurs des éléments : protection et action sociale pour les citoyens.

	2022	2021	2020	2019	2018	2017	2016	2015	2014
Acciones beneficio comunidad (más allá misiones encomendadas).	1.012	960	1.151	2.659	2.647	2.986	1.956	1.318	1.620
Acciones solidarias (voluntariado nivel individual hay constancia).	1.026	267	347	121	114	140	215	180	62
Actividades de acercamiento a la sociedad	247	499	503	482	340	316	105	904	142
Charlas en centros escolares	34.459	21.328	16.078	34.848	12.970	12.412	16.245	12.814	11.782
Acciones seguridad mayores	3.607	2.740	3.275	3.732	3.816	3.769	9.712	10.364	11.605
Colaboraciones convenios.	261	149	106	114	92	86	96	115	95
Servicios humanitarios	242.575	218.303	215.697	194.923	193.593	193.135	458.360	167.266	SD

Les données présentées ci-dessus (tableau 9) sont intéressantes car elles indiquent qu'au cours des neuf dernières années, 1 883 862 services humanitaires ont été réalisés ; 14 689 actions au profit de la communauté et 2 410 actions de volontariat. Sans compter d'autres activités de solidarité et de protection des personnes âgées et des mineurs. La démonstration que les personnes sont plus importantes que le capital dans l'économie sociale (Pedreño, 2024).

Ces données montrent que les services et actions humanitaires au profit de la société sont un plus. De plus, leur valeur financière est inestimable. Pour visualiser la valeur économique de ces actions, nous l'avons résumée en prenant l'exemple de l'Asociación Guardias Civiles Solidarios⁸ (ASGS). Le tableau 10 montre la valeur économique de ses actions au cours des 5 dernières années, données obtenues à partir des rapports annuels de l'ASGS.

	Actuaciones	Niños	Adultos	Alimentos (kg.)	Valor económico €
Memorias 2024	60	2.977	2.987	22.540	60.257
Memorias 2023	44	4.771	9.109	44.980	45.396
Memorias 2022	65	1.832	63.396	362.040	367.356, 21
Memorias 2021	54	2.419	5.346	13.210	52.000
Memorias 2020	138	2.017	13.251	8.262	38.482

Tableau 10
Évaluation économique des actions "Gardes civils solidaires"

Avec les données présentées dans les deux tableaux (8 et 9), nous entrons dans la discipline de l'économie sociale qui imprègne l'économie traditionnelle, la valeur du social (Díaz-Foncela et al., 2016) et l'institution de la Guardia Civil qui la soutient, grâce à son capital intellectuel. Ainsi, il est démontré que la valeur des services fournis a un impact positif sur l'économie sociale en poursuivant l'intérêt général économique et/ou social. Par conséquent, l'hypothèse 5 de notre recherche est confirmée :

H5 : La valeur économique sociale de l'institution influence l'économie sociale.

Enfin, nous avons analysé si l'économie sociale revient à l'institution, complétant ainsi l'objectif de notre recherche. Pour ce faire, nous avons analysé la confiance accordée à l'Institution par les citoyens, les institutions et diverses entités, réalisée par le Centre de Recherches Sociologiques (CIS) au cours de la période étudiée. Les résultats sont présentés dans le tableau 11 ci-dessous.

⁸En 2014, l'Asociación Guardias Civiles Solidarios (ASGC) a été fondée dans le but de canaliser les nombreuses actions individuelles du personnel bénévole.

Tableau 11
Valorisation de l'institution par la société espagnole

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Posición entre instituciones más valoradas	SD	FFCCSE	FFCCSE	FFCCSE	1ª	1ª	1ª	1ª	1ª	1ª

Comme on le voit, une valorisation positive est transmise à l'institution à travers la loyauté et la confiance que la société lui accorde. Le fait d'être reconnu comme une institution à valeur sociale augmente significativement sa réputation (Jeffrey et al., 2019 ; Maqbool et al., 2018). Au sein de l'institution, l'engagement acquis par les gardes civils envers la société favorise l'estime de soi et la motivation en luttant pour les droits de l'homme et les plus défavorisés (MS, 2023). Ces actions, programmes ou projets de volontariat sont alignés sur les objectifs de l'institution, tels que la protection et l'aide aux citoyens, ce qui la renforce.

En outre, leur structure consolidée et leur diversification ne servent pas seulement aux alliances qui génèrent des réseaux sociaux déjà établis, mais facilitent également les connexions entre les communautés et les individus éloignés les uns des autres (Álvarez & Berni, 2001). Sans oublier que la cohésion et la confiance qu'elles génèrent facilitent la diffusion interne et externe de la connaissance, qui est un élément intangible précieux dans l'économie (Nonaka & Takeuchi, 2021), ce qui la rend plus compétitive.

Conformément à ce qui précède, notre dernière hypothèse (H6) est vérifiée, ce qui conclut notre objectif de recherche.

H6 : L'économie sociale revient à l'institution.

5. CONCLUSIONS

La façon dont les entreprises gèrent le capital social est une caractéristique déterminante de notre époque. L'institution répond à la question posée par la nouvelle perspective économique, dans laquelle les organisations réfléchissent à leur contribution à la valeur de la société (Retolaza & Alzola, 2021). En analysant cette question à travers le CI de l'institution de la Garde civile, qui appartient au secteur public et est éminemment sociale, nous soutenons que, tout comme le capital ne crée pas de valeur par lui-même, les investissements dans ce capital ne le font pas non plus par eux-mêmes. Ce sont les capacités générées par les entreprises dans la gestion de ces actifs incorporels qui assureront la croissance économique (Hazan et al., 2021), par le biais des services.

L'institution, dans l'exercice de son activité de sécurité et de protection des citoyens, va plus loin en améliorant la vie des individus et/ou de la société dans son ensemble. Selon les données, cela est dû aux connaissances, aux relations, à la culture organisationnelle, à l'expérience et à la participation active des personnes qui composent l'institution. Nous en déduisons, grâce aux résultats obtenus dans le cadre de la recherche effectuée, que l'institution remplit l'un des objectifs énoncés dans le rapport du Partenariat pour l'inclusion économique de la Banque mondiale (2024), en étant capable d'évaluer ses programmes sociaux sur la base d'éléments probants clés.

Ses actions présentent un modèle inclusif, atteignant directement ceux qui en ont le plus besoin, générant une cohésion sociale grâce à la structure institutionnelle et à sa diversification. Il dispose d'une structure solide nécessaire à la collaboration avec d'autres organisations non gouvernementales, communautaires et du secteur privé (García-Flores & Palma, 2019), ce qui réduit les limitations de capacité.

Le caractère méritoire de l'institution, porté par son personnel, est une valeur sociale, qui est définie dans ce travail en montrant l'impact positif de ses actions sur la société. En la montrant comme un acteur actif, nous ouvrons une brèche dans le stéréotype de la sécurité en allant plus loin avec ses actions sociales, la protection de l'environnement et la biodiversité. Dans ce cas, nous avons présenté un modèle inclusif qui croit en la nécessité de la solidarité et de la coopération, qui supprime les barrières sociales et transforme les environnements difficiles. Ces actifs sont précieux pour l'institution, conformément aux critères VRIN de Barney (1991), car ils sont difficiles à imiter, à acheter ou à remplacer, ce qui leur confère un avantage concurrentiel.

Nous pensons que des données et des outils de mesure adéquats sont essentiels pour la mise en œuvre de politiques saines sur tout type de capital. Cela permet d'obtenir des informations et de montrer à toutes les parties intéressées l'investissement réalisé et les résultats obtenus (García-Porras, 2025), sous le prisme de la transparence. Dans cette recherche, des données quantitatives et qualitatives ont été collectées et analysées, poursuivant ainsi des lignes de recherche ouvertes basées sur des preuves concernant les différents écosystèmes qui accueillent l'économie sociale, remplissant ainsi l'un des objectifs de la stratégie industrielle fixée par l'UE (Carini et al., 2024).

Nous concluons par les contributions et les limites de cette étude. Les résultats montrent, d'une part, que les institutions appartenant au secteur public peuvent être impliquées dans les organisations non gouvernementales et privées en tant qu'agent de changement nécessaire, promouvant l'économie sociale. D'autre part, nous contribuons à l'application de l'étude de la gestion du CI dans une institution appartenant au secteur public, étant donné que l'étude du CI est davantage axée sur le secteur privé. Nous pensons qu'il est nouveau d'étudier la valeur sociale dans une institution qui est souvent étudiée d'un point de vue juridique ou opérationnel.

En ce qui concerne les limites rencontrées, il convient de mentionner que le fait que les données soient basées sur des documents institutionnels pourrait générer un biais de source unique. Dans le même ordre d'idées, les indices des éléments obtenus à partir du CI n'ont pas été pondérés, ce qui minimise l'importance relative qu'ils peuvent avoir pour le groupe spécifique d'experts en économie sociale. Des recherches supplémentaires dans ce domaine seraient nécessaires pour améliorer notre compréhension de cette question. Par conséquent, une future ligne de recherche pourrait renforcer cette étude en utilisant des opinions d'experts et d'autres perceptions externes et en envisageant l'utilisation d'indices pondérés.

RÉFÉRENCES BIBLIOGRAPHIQUES

- Alvarez, S. A. et Barney, J. B. (2001). How entrepreneurial firms can benefit from alliances with large partners". *Academy Of Management Perspectives*, 15(1), 139-148. <https://doi.org/10.5465/ame.2001.4251563>
- Aramburu, N., Sáenz, J. et Rivera, O. (2005). Gestion des connaissances : aspects méthodologiques et empiriques. Document de travail. Saint-Sébastien, Université de Deusto EST.
- Arteaga A. L., Ojeda, J. F., et Alvarez D. G. (2020). Trajectoire et stratégies de l'entrepreneuriat chez les femmes. *aDResearch ESIC International Journal Of Communication Research*, 22(22), 176-195. <https://doi.org/10.7263/adresic-022-10>
- Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99-120. <https://doi.org/10.1177/014920639101700108>
- Bellucci, M., Marzi, G., Orlando, B. et Ciampi, F. (2021). A review of emerging themes and future trends. *Journal of intellectual capital*, 22(4), 744-767. <https://doi.org/10.1108/JIC-10-2019-0239>
- Bini, L., Bellucci, M. et Giunta, F. (2017). Intégrer la durabilité dans la divulgation du modèle d'entreprise : preuves de l'industrie minière britannique. *Journal of Cleaner Production*, 171, 1161-1170. <https://doi.org/10.1016/j.jclepro.2017.09.282>
- Briñez M. E. (2021). Information technology : An empowering tool for managing intellectual capital ? *Revista de Ciencias Sociales* 27(1), 180-192. <https://dialnet.unirioja.es/servlet/articulo?codigo=7817690>
- Bontis, N. (2002). Intellectual capital disclosure in Canadian corporations. *Journal of Human Resource Costing and Accounting*, 7(1-2), 9-20.
- Bueno E. J. et Merino C. (2007). Le capital intellectuel et la création d'entreprises dans la société. *Encuentros multidisciplinares*, (9)26, 37-46. <https://dialnet.unirioja.es/servlet/articulo?codigo=2324790>
- Bueno, E. J., Salmador, M. P. et Merino, C. (2008). Genèse, concept et développement du capital intellectuel dans l'économie de la connaissance : une réflexion sur le modèle Intellectus et ses applications. *Studies in Applied Economics*, 26(2), 43-63. <https://www.redalyc.org/pdf/301/30113187003.pdf>
- Burt, R. S. (2004). Brokerage and Closure : An Introduction to Social Capital.
http://ronaldburt.com/research/files/B&C_Introduction.pdf
- Cañibano L., Sánchez, P., García-Ayuso, M. et Chaminade, C. (2002). Projet MERITUM. Lignes directrices pour la gestion et la diffusion de l'information sur les actifs incorporels (Rapport sur le capital intellectuel). Fondation Vodafone.
<https://dialnet.unirioja.es/servlet/libro?codigo=448252>
- Carini, Ch., Galera, G., Tallarini, G., Chaves, A., Sak, B. & Schoenmaeckers, J., (2024). *Analyse comparative des performances socio-économiques de l'économie sociale de l'UE*. Commission européenne.

https://eisma.ec.europa.eu/news/study-benchmarking-socio-economic-performance-eu-social-economy-now-published-2024-09-19_en

Commission européenne (CE, 2006). Reporting intellectual capital to augment research, development and innovation in SMEs : report to the Commission of the High Level Expert Group on RICARDIS (Commission européenne. Direction générale de la recherche ed.). Luxembourg : Office des publications officielles des Communautés européennes.

<https://op.europa.eu/es/publication-detail/-/publication/60cbf27c-5552-429f-a077-44135a97cc27/language-en>

Chen, Y. S. (2008). The positive effect of green intellectual capital on competitive advantages of firms. *Journal of Business Ethics*, (77)3, 271-286. <https://doi.org/10.1007/s10551-006-9349-1>

Chen, H., Shih A. & S. Y. Yang, (2009). The Role of Intellectual Capital in Knowledge Transfer (Le rôle du capital intellectuel dans le transfert de connaissances). *IEEE Transactions on Engineering Management*, (56)3, 402-411.

<https://ieeexplore.ieee.org/abstract/document/5072284>

Codina, L., Morales-Vargas, A., Rodríguez-Martínez, R. et Pérez-Montoro, M. (2020). Utilisation de Scopus et Web of Science pour la recherche et l'évaluation en communication sociale. Analyse comparative et caractérisation. *Index.Comunicación/Index Comunicación*, 10(3), 235-261. <https://doi.org/10.33732/ixc/10/03usodes>.

Davenport, T. et Prusak, L. (2001). *Knowledge in action*. Buenos Aires : Prentice Hall. Argentine.

De Castro, G. et García-Muiña, F. E (2003). Hacia una visión integradora del capital intelectual de las organizaciones. Concept et composantes. *ICE Economic Bulletin, Spanish Commercial Information*, 2756, 7-16. <https://dialnet.unirioja.es/servlet/articulo?codigo=303756>

Delgado, M., Navas, J.E., Martín. G. & López, P. (2008). L'innovation technologique dans le cadre du capital intellectuel. Rapport de recherche 04/2008. Université Complutense de Madrid.

Demartini, C. et Trucco, S. (2016). Does Intellectual Capital Disclosure Matter for Audit Risk ? Evidence from the UK and Italy. *Sustainability*, 8(9), 867. <https://doi.org/10.3390/su8090867>

Díaz B. F. et Lejarriaga G. (2019). Présentation de la monographie : Entrepreneuriat social et employabilité. *REVESCO. Revista de Estudios Cooperativos*, 129, 9-15. <https://doi.org/10.5209/REVE.62962>

Díaz-Foncela M., Marcuello S. et Monreal G. (2016). Économie sociale et économie collaborative : Fit et potentialités. *Industrial Economics*, 402, 27-35 <https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/402/D%C3%8DAZ%20FONCELA,%20MARCUELLO%20Y%20MONREAL.pdf>

Dumay, J., Bernardi, C., Guthrie, J. et Demartini, P. (2016). Integrated reporting : A structured literature review. *Accounting Forum*, 40(3), 166-185. <https://doi.org/10.1016/j.accfor.2016.06.001>

- Edvinsson, L. et Malone, M.S. (1999). Le capital intellectuel. Barcelone : Gestión, 2000.
- Fernández , D. J. Guevara, G. D. , Dávila T. L. et Cruz, J. J. (2022). Intellectual capital as a factor of organizational performance in Micro and Small Enterprises (Le capital intellectuel comme facteur de performance organisationnelle dans les micro et petites entreprises). *Journal of Research in Communication and Development*, 13(1), 63-73. <https://doi.org/10.33595/2226-1478.13.1.595>
- Fernández-Solís, C., González-Ramírez, M. R., et Gascó-Gascó, J. (2025). L'intention d'adoption de l'analyse des ressources humaines et son impact sur la performance organisationnelle : une approche théorique. *INNOVA Research Journal*, 10(1), 93-111. <https://doi.org/10.33890/innova.v10.n1.2025.2706>
- Garanina T., Hussinki H. et Dumay J. (2021). Accounting for intangibles and intellectual capital : A literature review from 2000 to 2020, *Accounting & Finance*, à paraître. <https://doi.org/10.1111/acfi.12751>
- García-Flores, V. et Palma Martos, L. P. (2019). L'innovation sociale : facteurs clés pour son développement dans les territoires. CIRIEC-Espagne Revista de Economía Pública Social y Cooperativa, 97, 245-278. <https://doi.org/10.7203/ciriec-e.97.14148>
- García-Flores, V. et Palma Martos, L. P. (2020). Entités du troisième secteur et innovation sociale. Éléments de caractérisation et facteurs de réussite. *REVESCO Journal of Cooperative Studies*, 136, e71861. <https://doi.org/10.5209/reve.71861>
- García-Porras, B. (2025). Présentation du rapport statistique CIRIEC, Euricse et Spatial Foresight. Benchmarking the socio-economic performance of the EU Social Economy. <https://ciriec.es/noticias/el-nuevo-informe-de-euricse-ciriec-internacional-y-spatial-foresight-impulsado-por-la-comision-europea-cifra-en-115-millones-las-personas-empleadas-en-la-economia-social-en-la-ue/>
- Grant, R. M. (1996). Toward a Knowledge-Based Theory of the Firm. *Strategic Management Journal*, 17, 109-122. <https://doi.org/10.1002/smj.4250171110>
- Guthrie, J. et Abeysekera, I. (2006). Content analysis of social, environmental reporting : What is new ?, *Journal of Human Resource Costing & Accounting*, 10(2), 114-126. <https://doi.org/10.1108/14013380610703120>
- Hazan, E., Smit, S., Woetzel J., Cvetanovski, B., Krishnan, M., Gregg, B., Perrey J. et Hjartar, K. (2021). Rendre tangible l'intangible. The future of grow and productivity ? McKinsey Global Institute. <https://doaj.org/article/faecfbdaace64e669c135ccadc104776>
- Haarhaus, T. et Liening, A. (2020). Construire des capacités dynamiques pour faire face à l'incertitude environnementale : le rôle de la prospective stratégique. *Technological Forecasting and Social Change*, 155. <https://doi.org/10.1016/j.techfore.2020.120033>
- Jeffrey, S., Rosenberg, S. et McCabe, B. (2019). Comportements de responsabilité sociale des entreprises et réputation des entreprises. *Social Responsibility Journal*, 15(3), 395-408. <https://doi.org/10.1108/SRJ-10.11-2017-0255>
- Johnson, W.H.A. (1999). An integrative taxonomy of intellectual capital : Measuring the stock and flow of intellectual capital components in the firm (taxonomie intégrative du capital intellectuel : mesure du stock et du flux des composants du

- capital intellectuel dans l'entreprise). *International Journal of Technology Management*, 18(5-8), 562-575.
- Lev, B. (2001). *Intangibles : Management, Measurement, and Reporting*. Washington DC : Brookings Institution Press. <http://www.jstor.org/stable/10.7864/j.ctvcj2rf2>
- Li, X., Nosheen, S., Haq, N. U. et Gao, X. (2020). Value creation during fourth industrial revolution : Use of intellectual capital by most innovative companies of the world (Création de valeur pendant la quatrième révolution industrielle : utilisation du capital intellectuel par les entreprises les plus innovantes du monde). *Technological Forecasting And Social Change*, 163, 120479. <https://doi.org/10.1016/j.techfore.2020.120479>
- López P., Martín de Castro, G., et Navas, J.E. (2004). Une approche des relations entre les éléments du capital intellectuel dans les organisations. *Bulletin économique de la CIE* (2817). <https://www.revistasice.com/index.php/BICE/article/view/3626/3626>
- Maqbool, S., Rasool, H., & Ahmad, S. (2018). Responsabilité sociale des entreprises et performance financière : une analyse empirique des banques indiennes. *Future Business Journal*, 4(1), 2314-7210. <https://doi.org/10.2139/j.fbj.2017.12.002>
- Magau, M. D., Roodt, G. et van Zyl, G. (2021). A measurement scale for assessing intellectual capital disclosure. *Journal of HumanResource Management*, 19, 1-14. <https://doi.org/10.4102/sajhrm.v19i0.1645>
- Merino C., Alonso, M., González, N., & Plaz, R. (2018). La gestion des connaissances dans les organisations du secteur nucléaire. Université nationale d'enseignement à distance (UNED).
- Ministère de l'intérieur (GC, 2023). Rapport de durabilité 2023 de la Guardia Civil. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/memoria-RSC-Sostenibilidad-de-la-Guardia-Civil/Memoria-sostenibilidad-GC_126230302_pdfWEB.pdf
- Ministère du travail et de l'économie sociale (MITES). Informe de evolución y Tendencias en el ámbito de la Economía Social (2023). Confédération espagnole des entreprises de l'économie sociale (CEPES). https://www.fundae.es/docs/default-source/publicaciones-y-evaluaciones/publicaciones-econom%C3%ADa-social/1-1-evoluci%C3%B3n-y-tendencias-de-la-ec-social_2023.pdf
- Mohdzaini, H. (2021). Technology and the future of work : How artificial intelligence (AI) robots and automation are shaping the world of work, m the ethical considerations and the role of people professionals. CIPD. <https://www.cipd.org/uk/knowledge/factsheets/emerging-future-work-factsheet/>
- Moreiro J. A., Morato J., Sánchez S. y Rodríguez B. A., (2006). Catégorisation des concepts dans l'analyse de contenu : sa signalisation de la rhétorique classique aux cartes thématiques. *Investigación Bibliotecológica : Archivonomía, bibliotecología e información*, 20(40). <https://doi.org/10.22201/iibi.0187358xp.2006.40.4097>
- Navarro González A. et Medina Jiménez, A., (2024). Relación del Capital intelectual con el capital humano, estructural y relacional. *Transcender Contabilidad y Gestión*, 9(26), 100-127. <https://doi.org/10.36791/tcg.v9i26.260>

- Nonaka, I. et Takeuchi, H. (1995). *The knowledge creating company (L'entreprise créatrice de connaissances)*. New York : Oxford University Press.
- Nonaka, I. et Konno, N. (1998). The Concept of Ba : Building a Foundation for Knowledge Creation. *California Management Review*, 40, 40-54. <https://doi.org/10.2307/41165942>
- Nonaka, I. et Takeuchi, H. (2021). Humanizing strategy. *Long Range Planning*, 54(4), 102070. <https://doi.org/10.1016/j.lrp.2021.102070>
- Oliveira, M., Curado, C., Balle, A. R. et Kianto, A. (2020). Knowledge sharing, intellectual capital and organisational results in SMES : are they related ? *Journal of Intellectual Capital*, 21(6), pp. 893-911. <https://doi.org/10.1108/JIC-04-2019-0077>
- Organisation de coopération et de développement économiques (2006). Créer de la valeur à partir des actifs intellectuels. Réunion du Conseil de l'OCDE au niveau des ministres.
- Pedreño, J., (2024). L'économie sociale et les objectifs de l'UE 2024-2029. *Europe Social Economy*. <https://www.socialeconomy.eu.org/2024/10/22/great-sucess-of-the-event-the-social-economy-and-the-eu-2024-2029-objectives/>
- Petty, R. et Guthrie, J. (2000). Intellectual capital literature review. *Journal Of Intellectual Capital*, 1(2), 155-176. <https://doi.org/10.1108/14691930010348731>
- Porter, M. (1996). Qu'est-ce que la stratégie ? *Harvard Business Review* 74(6), 61-78. https://iqfystage.blob.core.windows.net/files/CUE8taE5QUKZf8ujfYlS_Readin+1.4.pdf
- Retolaza, J. et Alzola, M. (2021). Applying social value in organisations. *Bulletin of Economic Studies*, 76(232), 19-22. <https://doi.org/10.18543/bee.2383>
- Rideg, András, Szerb, László et Róza Varga, Anna (2023). The role of intellectual capital on innovation : Evidence from Hungarian SMEs (Le rôle du capital intellectuel dans l'innovation : preuves issues des PME hongroises). *Tec Empresarial*, 17(2), 1-19. https://www.researchgate.net/publication/370608181_The_role_of_intellectual_capital_on_innovation_Evidence_from_Hungarian_SMEs
- Roos, J. (2001). *Le capital intellectuel : la valeur immatérielle de l'entreprise*. Barcelone : Paidós.
- Sánchez-Espada J., Martín S., Bel P. et Lejarriaga G. (2018). Éducation et formation à l'entrepreneuriat social : caractéristiques et création de valeur sociale durable dans les projets d'entrepreneuriat social. *REVESCO. Revue d'études coopératives*, 129, 16-38. <http://dx.doi.org/10.5209/REVE.62492>
- Secundo, G., Ndou, V., Del Vecchio, P. et De Pascale, G. (2020). Développement durable, capital intellectuel et politiques technologiques : une revue structurée de la littérature et un programme de recherche futur. *Prévision technologique et sociale* <https://doi.org/10.1016/j.techfore.2020.119917>
- Stratone, M. (2023). A Bibliometric Analysis of the Role of the Intellectual Capital in the Organizational Agility and Performance (Analyse bibliométrique du rôle du capital intellectuel dans l'agilité et la performance organisationnelles).

Proceedings Of The International Conference On Business Excellence, 17(1), 1275-1285. <https://doi.org/10.2478/picbe-2023-011>

Steward, T. (1997). La nouvelle richesse des organisations : le capital intellectuel Buenos Aires : Ediciones Granica S.A.

Suciu, M., & Nășulea, D. (2018). Le capital intellectuel et l'économie créative comme moteurs clés de la compétitivité vers un développement intelligent et durable : défis et opportunités pour les communautés culturelles et créatives. In : La gestion du capital intellectuel comme moteur de la durabilité. https://doi.org/10.1007/978-3-319-79051-0_5

Sumedrea, S. (2013). Intellectual Capital and Firm Performance : A Dynamic Relationship in Crisis Time (Capital intellectuel et performance de l'entreprise : une relation dynamique en temps de crise). *Procedia Economics And Finance*, 6, 137-144. <https://www.sciencedirect.com/science/article/pii/S2212567113001251?via%3Dihub>

Teece, D.J., Pisano, G. et Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533.

Thum-Thysen, A., Voigt, P. et Weiss, C. (2021). Réflexions sur les complémentarités dans la formation et la production de capital : actifs tangibles et intangibles à travers l'Europe. Commission européenne/Economie européenne [en ligne] https://economy-finance.ec.europa.eu/document/download/3ddd17a1-0d58-4614-a363-90a9e6a12e9c_en?filename=dp152_en.pdf

Wang, C.N., Chang, Y.L., Huang, Q.H. et Wang, C.H. (2011). Évaluation de la gestion du capital intellectuel pour l'industrie pharmaceutique taïwanaise : utilisation de GRA et MPI. *African Journal of Business Management* 5(7), 2950-2958.

<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=78a492920f297eb118e7972ef4ad52ce99ec2355>

Groupe de la Banque mondiale (2024). Rapport annuel 2024. <https://openknowledge.worldbank.org/bitstreams/91a20260-c3c4-4ed7-a488-d7dd8d419c8a/download>

Xu, J. et Wang, B. (2018). Le capital intellectuel, la performance financière et la croissance durable des entreprises : preuves de l'industrie manufacturière coréenne. *Sustainability*, 10(12), 4651. <https://doi.org/10.3390/su10124651>.

Zheng S., Zhang W., Wu X. & Du J. Know ledge-based Dynamic capabilities and innovation in networked environments. *Journal of Knowledge Management* 15(6), 1035-1051.

Annexe I

Tableaux 4-6 : Unités d'échantillonnage et définition des dimensions du QI dans l'institution

ELEMENTOS DIMENSIÓN CAPITAL HUMANO		
Códigos	Unidad Muestral	Definición
CHIDENTIDAD	Pertenencia y compromiso.	Identificación de las personas como guardias civiles dentro de la Institución.
CHMOTIVACION	Automotivación	Los impulsos conscientes que hacen a los guardias civiles conseguir desempeñar el servicio con excelencia.
CHSATISFACCION	Satisfacción	Forma de participar en el desempeño de su trabajo y comportamientos de los guardias civiles en la Institución. Evaluación desempeño.
CHCREATIVO	Creatividad. Cultura innovadora	Creación de ideas nuevas y aplicables al desempeño del servicio. La forma de impulsar los pensamientos nuevos, ideas y actitudes por la Institución para generar nuevas formas de actuación o una mejora de las existentes.
CHEDUCACION	Educación reglada.	Conocimientos explícitos que posee en general los guardias civiles.
CHESPECIALIDAD	Formación especializada.	Conocimientos específicos de una especialidad concreta o trabajo técnico en la Institución
CHUNIVERSITARIO	Inversión en formación Universitaria.	Centro Universitario Guardia Civil (CUGC).
CHFORMACION	Formación interna.	Conocimientos adquiridos mediante programas, jornadas, talleres, y todos los cursos de formación que comprenden la capacitación y promoción interna en las Academias y en el Centro Universitario de la GC.
CHEXPERIENCIA	Experiencia.	Conocimientos adquiridos mediante el desempeño realizado en la Institución.
CHDESARROLLO	Desarrollo personal.	Conocimientos adquiridos informalmente en la Institución. Personas que promocionan. Promoción interna.
CHAPRENDIZAJE	Aprendizaje	Adquisición de nuevos conocimientos. Jornadas PATIO Y SIO.
CHCIVIL	Colaboración, personal civil.	Capacidad de trabajar con otras personas: compañeros, personal administraciones públicas. Personal civil funcionariado.
CHCONCILIA	Conciliación vida familiar profesional	Favorecer el equilibrio entre la vida familiar y la laboral a los guardias civiles. Compatibilizar la vida profesional y familiar.
CHLIDERAZGO	Liderazgo.	Guiar y mover a los compañeros hacia el desempeño de un servicio con excelencia y otras personas relacionadas con el servicio.

ELEMENTOS DIMENSIÓN CAPITAL ESTRUCTURAL

Códigos	Unidad Muestral	Definición
CECULTURA	Homogeneidad cultural.	Aceptación de los valores de la Guardia Civil.
CECLIMA	Clima social-laboral.	Ambiente generado en la unidad, departamento o equipo de trabajo. Índice de clima social.
CEIGUALDAD	Sensibilidad género. Igualdad.	Introducción de la perspectiva de género en la Institución. Igualdad de condiciones entre hombres y mujeres acceso mismo puesto bajo las mismas condiciones e iguales requisitos
CESTRUCTURA	Diseño organizativo. Plantilla. Delimitación competencias	Estructura de la Institución que establece las relaciones laborales. Distribución. Competencias funcionales.
CEDESARROLLO	Desarrollo organizativo.	Acontecimientos que propician adaptación a las situaciones actuales. Regulación de Jornadas y horarios en general.
CERUTINAS	Pautas organizativas. Procedimientos establecidos y sistemas.	Procedimientos y rutinas establecidos o nuevas competencias para mejorar la Institución. Mejora de las funciones a desempeñar por los guardias civiles, mejorando su calidad profesional y aumentando su motivación.
CERELACIONINT	Explicación de la estrategia a su personal.	Procesos dirigidos a explicar a los componentes de la Institución su Estrategia, visión, misión e innovación. Introducción de algo nuevo o modificación de lo anterior que provoque un mejor desempeño en el servicio.
CECRIMINAL	Actuaciones, denuncias e infracciones administrativas.	Procesos dirigidos a explicar, numerar y contextualizar las detenciones, denuncias e infracciones administrativas.
CEPROVEEDORES	Contratación proveedores.	Conjunto de procesos de proveedores, alineados a los valores de la Institución. Contratación pública socialmente responsable (CPSR). Orientado a los riesgos laborales, reciclaje y medio ambiente.
CEINVERSIONIDI	Inversión I+D+i. Dominios de sus sedes electrónicas.	Inversión económica en investigación y desarrollo. Gastos elaborados por su funcionamiento al desarrollar acciones innovativas, conferidas como espacios virtuales de uso exclusivo por la Institución. Dominios internet.
CEPERSONALIDI	Personal I+D+i.	Plantilla de plena dedicación a investigación y desarrollo.
CEPROYECTOSIDI	Proyectos I+D+i. Programa Marco UE. Programa Horizonte 2020.	Trabajos realizados relacionados con la innovación y el desarrollo. Proyectos generados en concordancia con el proceso innovativo con otras organizaciones o de forma independiente.
CEINFRAESTRUCTURA	Infraestructuras y material.	Mantenimiento de las instalaciones. Inversión en instalaciones e infraestructuras.
CEEQUIPOPOLICIAL	Equipamiento policial. Dotación tecnologías de producción.	Productos y herramientas adecuadas a las necesidades particulares de la Institución. Conjunto de equipos tecnológicos necesarios para el cumplimiento de un servicio.
CEINNGEST	Innovación de gestión. Innovación de modelo de Institución.	Herramientas nuevas y procedimientos compartidos en la Institución que impulsan la innovación. Transformación digital.
CECOMUNICACIONGC	Comunicación interna Relaciones asociaciones. Consejo.	Sistemas informáticos, telecomunicaciones útiles funcionamiento de la Institución. Facilidad y buena actitud en la transmisión de los conocimientos e información para la ejecución de un servicio con las personas adecuadas para ello. Atención al guardia civil.
CEMARCA	Marcas registradas. Imagen de la GC	Marca, logo y emblemas en la Institución. Referencia a los uniformes.
CELICENCIAS	Licencias forenses, subscriptores.	Procesos por el que se comparte una parte de los procesos y conocimientos de la Institución. Convenios con otras administraciones y universidades.
CESECRETO	Protección de datos.	Todos los considerados por la Institución como tales. Protección de datos (ciudadanos).
CEPATENTES	Información patentes.	Base de datos registren cantidad y uso de patentes empleadas por la Institución.
CETECNOEXT	Conocimiento actividad tecnológica competencia.	Bases de datos e información disponible sobre los avances en I+D de los competidores.
CETECNONEW	Información sobre líneas investigación y tecnología emergente.	Bases de datos de información sobre tecnología emergente que afecte a la Institución. Conocimiento posibles asociaciones con empresas para I+D.
CETECLIC	Localización tecnología sobre la que buscar licencias	Fuentes de datos sobre tecnologías útiles para ser desarrolladas en la Institución.
CEFLEXIBILIDAD	Flexibilidad y adaptabilidad.	Comportamiento favorable hacia el cambio por las situaciones derivadas del servicio o de la Institución.
CETALENTOS.	Antigüedad y fidelización de los guardias civiles.	Permanencia de los empleados basada en políticas de retención y atracción de guardias civiles que aportan valor a la Institución. Situaciones.

ELEMENTOS DIMENSIÓN CAPITAL RELACIONAL

Códigos	Unidad Muestral	Definición
CRCIU	Base ciudadanos.	Ciudadanos en general.
CRLEALCIU	Lealtad ciudadanos.	Grado de fidelidad que procesan los ciudadanos a la Institución. Primera opción en seguridad.
CRSATISFACCION	Satisfacción ciudadanos. Seguridad pública.	Grado de eficacia que el ciudadano percibe en la cumplimentación de un servicio y en general con la Institución. Felicitaciones atención al ciudadano.
CRQUEJAS	Quejas, reclamaciones y sugerencias ciudadanos.	Quejas recibidas por la prestación de un servicio y sugerencias. Atención a la ciudadanía. Oficina de Información y Atención al Ciudadano(OIAC). Puntos de Atención Especializada (PAEs).
CRPROTCIU	Procesos relación ciudadanos. Protocolos ciudadanos.	Protocolos de actuación y comportamiento con los ciudadanos. Turismo seguro. Trata de seres humanos (TSH). Mayores seguros. VdG. Menores. Víctimas de terrorismo.
CRESTADO	Relaciones Estado y UE. Accionistas e inversiones institucionales.	Grado de inversiones; recursos disponibles; presupuestos.
CRIADMINISTRACION	Relaciones Institución mercado. Relaciones con otros grupos de interés Administración.	Relaciones con otros grupos de interés de la Institución. Administración general ACCEDA; Firma digital. Partidos políticos. Firma convenios administraciones.
CRCAPITALEXTERIOR	Relaciones participación empresarial.	Capital de la Institución en otras entidades.
CRALIANZAS	Base aliados.	Alianzas con otras instituciones dentro de su área de seguridad. Relacionados con la creación de conocimiento, y su transferencia impulsando la innovación.
CRALIANZASESTABLES	Solidez alianzas. Servicios conjuntos. Estabilidad alianzas y formalización.	Formas establecidas de cooperación con policías misma área de seguridad. Innovación internacional. Nuevas formas en otros países que contribuyan al desarrollo o diversificación de la Institución o sus competencias. Misiones encomendadas por el Ministerio de Defensa.
CRALIANZASBENEFICIO	Beneficio alianzas. Resultados obtenidos alianzas.	Generación de beneficios de las alianzas establecidas. Ayuntamientos Seguridad Ciudadana y Seguridad Vial. Protección civil.
CRCONCOMPETENCIA	Conocimiento competidores.	Conocimiento otras policías en la compartición de las competencias de seguridad.
CRPRIVADA	Relaciones seguridad privada.	Grado beneficios obtenido relaciones con otros grupos de interés. Seguridad privada.
CRCERTICAL	Certificaciones y sistemas calidad.	Certificados de calidad otorgados a la Institución. Premios (SEPRONA); Igualdad.
CRREDES	Portal guardia civil exterior. Información divulgada redes.	Canales de comunicación en la Institución basado en la tecnología. Notas de prensa e información comparte Institución en Redes Sociales. Información pública.
CRADMINISTRACION	Colaboración Adm. Públicas. Cooperación para el desarrollo.	Cooperación con otras administraciones nacionales e internacionales de la Institución. Ministerios. Compras públicas innovadoras firma de Convenios con otras administraciones.
CRMEDIOS	Relaciones medios comunicación convencionales.	Exposición de la institución medios de comunicación. TVE; radio; periódicos. Medios más convencionales.
CRDEFENSAMBIENTE	Relaciones instituciones defensa medioambiental.	Grado de efectividad con otros grupos dedicados a la defensa del medioambiente.
CRVERDE	Códigos y certificaciones medio ambientales.	Procedimientos y protocolos establecidos interiorizados por la Institución en la defensa del medioambiente.
CRMERCADO	Relaciones instituciones mercado trabajo.	Relaciones institución con el mercado laboral. Contribución al tejido empresarial Oferta empleo público (OEP).
CRCODIGOCON	Código de conducta.	Nuestro código es normativo. Normas explícitas establecidas de comportamiento recogidas en el Reglamento. Código Penal Militar.
CRACSOCIAL	Acción social al ciudadano. Preocupaciones sociales	Espíritu Benemérito. Comportamiento adecuado y correcto del personal especialmente con los ciudadanos en el desempeño del servicio. Responsabilidad con la sociedad, desarrollo económico, solidaridad e integración social.
CRBUENGOBIERNO	Dirigidos a los ciudadanos. Buen gobierno.	Procesos dirigidos a la catalogación de los ciudadanos, sus riesgos y necesidades. Código buen gobierno de la AGE. Difusión de buenas prácticas. Transparencia, responsabilidad y eficacia con todos los grupos de interés. Compromiso adquirido voluntario por la Institución como forma de rendir cuentas a la sociedad a la que sirve.

Annexe II

Exemples de calcul de l'indice d'un élément, appartenant à chaque catégorie.

Categoría Capital Humano

Elemento: *CHEducación*.

$$I \text{ CHEducación} = 1/14 \sum_{i=1}^{14} j = I \text{ CHEducación cuanti} + I \text{ CHEducación cualit} + I \text{ CHEducación gráfico}$$



Categoría Capital Estructural

Elemento: *CERutinas*.

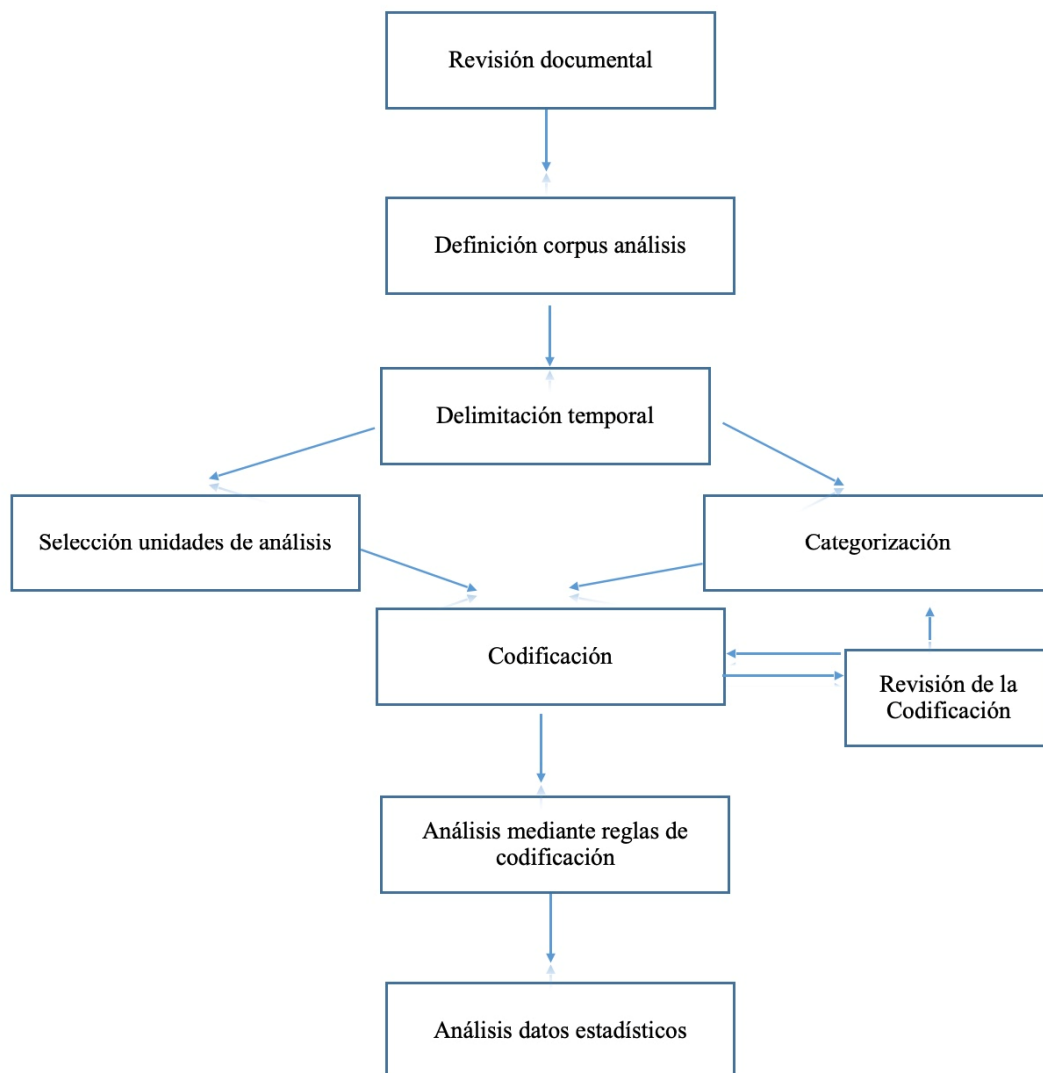
$$I \text{ CERutinas} = 1/25 \sum_{i=1}^{25} j = I \text{ CERutinas cuanti} + I \text{ CERutinas cualit} + I \text{ CERutinas gráfico}$$

Categoría Capital Relacional

Elemento: *CRLealcu*.

$$I \text{ CRLealcu} = 1/23 \sum_{i=1}^{23} j = I \text{ CRLealcu cuanti} + I \text{ CRLealcu cualit} + I \text{ CRLealcu gráfico}$$

Annexe III
Phases développées dans l'analyse de contenu





III.- REVUE DE LA JURISPRUDENCE



Revue de la jurisprudence

EXAMEN DE LA JURISPRUDENCE 2E CHAMBRE COUR SUPREME

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

Javier Ignacio Reyes López
Magistrat du 46e tribunal d'instruction de Madrid
Diplôme d'études approfondies (DEA)
ji.reyes@poderjudicial.es

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

Citation recommandée : Reyes, J. I. (2025). Reseña de jurisprudencia Sala 2ª Tribunal Supremo. *Revista Logos Guardia Civil*, 3(2), p.p. 295-320.

Licence : Cet article est publié sous la licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Dépôt légal : M-3619-2023

NIPO en ligne : 126-23-019-8

ISSN en ligne : 2952-394X

EXAMEN DE LA JURISPRUDENCE COUR SUPREME DE LA DEUXIEME CHAMBRE

Résumé: STS 350/2025, du 10 avril. Notion de partie intéressée dans une recherche de logement. 2 - STS 358/2025, du 10 avril 2025. Nouvelles criminelles transférées en Espagne par une autorité judiciaire étrangère et poursuite de l'enquête dans notre pays avec de nouvelles investigations. 3 - STS 324/2025, du 7 avril 2025. Conservation des données de communication. 4 - STS 294/2025, du 28 mars 2025. Principe d'insignifiance et de toxicité dans les infractions contre la santé publique. 5 - STS 8/2025, Section pénale 3^a, du 2 avril 2025. Délit de destruction à des fins terroristes. 6 - STS 308/2025, du 2 avril 2025. Enquête policière en Espagne découlant de la connaissance d'un OEB délivré par les autorités judiciaires d'un autre pays pour une autre infraction pénale. Présence de détenus lors d'une perquisition. 7 - STS 295/2025, du 28 mars 2025. Délit de harcèlement, "stalking". 8 - STS 284/2025, du 27 mars. Abus sexuel sur une personne de 17 ans à l'intelligence limite. Préjudice moral.

1 - STS 350/2025, du 10 avril. Notion de partie intéressée dans le cadre d'une recherche de logement .¹

Contexte factuel.

Le Juzgado de Instrucción n° 5 de Marbella a ouvert la procédure abrégée n° 104/2018 pour un crime présumé contre la santé publique à l'encontre de Noelia, entre autres, qui, une fois conclue, a été renvoyée pour jugement à la 1ère section de la Cour provinciale de Malaga. La procédure abrégée n° 1004/2019 a été ouverte le 17 mai 2021 et le tribunal a rendu la sentence n° 233/2021, dans laquelle il a déclaré comme prouvé que "....". Compte tenu des preuves, il est expressément et catégoriquement déclaré comme prouvé que le groupe de criminalité urbaine du commissariat du CNP de Marbella a effectué une opération de surveillance pour détecter la vente de substances dans la zone xx de Marbella, située entre la zone industrielle Ermita et le boulevard de l'avenue José Manuel Valles et à côté d'une école, un point fréquent et connu pour son conflit et pour être un point de vente et de consommation de drogues. Ils ont eu connaissance de l'existence du clan "Chatos" dédié à la vente de stupéfiants par le biais des propriétés situées dans ce bidonville, car ils savaient que leurs résidents pouvaient être impliqués dans la vente de stupéfiants, étant donné qu'il y avait un flux quotidien de personnes effectuant des visites de courte durée. À la suite de la surveillance, de l'observation exhaustive, de l'interception et de la saisie successive, au moyen de rapports, de stupéfiants provenant de personnes venues spécifiquement acheter dans les maisons faisant l'objet de l'enquête, les rapports suivants sont recueillis [...] et par la suite, sur la base de la demande de la police, par le tribunal d'instruction n° 5 de Marbella, une ordonnance a été rendue le 4 juin 2018 autorisant l'entrée et la perquisition, entre autres,

¹ STS 350/2025, section pénale 1 du 10 avril. Publié sur le site du Centre de documentation judiciaire, CENDOJ, (ROJ : STS 1701/2025 - ECLI:ES:TS:2025:1701), recours n° 7569/2022. Rapporteur, M. Eduardo de Porres Ortiz de Urbina.

dans les différentes maisons dans lesquelles des substances stupéfiantes ont été saisies et les personnes enquêtées ont été arrêtées [...]".

Base juridique.

Le Tribunal suprême est saisi d'un pourvoi en cassation contre l'arrêt n° 197/2022, du 14 juillet 2022, rendu par la chambre civile et pénale du Tribunal supérieur de justice d'Andalousie, Ceuta et Melilla, qui a rejeté le recours formé contre l'arrêt n° 233/2021, du 17/05/2021, de la 1ère section de l'Audiencia Provincial de Malaga, portant condamnation pour délit contre la santé publique. Des quatre personnes condamnées, une seule a interjeté appel.

Le premier moyen fait valoir que l'arrêt attaqué a violé le droit au respect de la vie privée au domicile de , article 18.2 CE, et le droit à un procès assorti de toutes les garanties reconnues à l'article 24.2 de la Constitution.

Elle affirme qu'elle était en détention au moment des perquisitions et qu'elle ne pouvait être présente que dans l'une d'entre elles (la maison qu'elle quittait lorsqu'elle a été arrêtée) et non dans les autres maisons, pour lesquelles un lien criminel lui a été attribué.

La défense comprend que la présence de l'intéressé est une exigence inexcusable pour une perquisition à domicile conformément à art. 569 LECrim, étant nulles et non avenues les perquisitions à domicile qui ne respectent pas cette exigence lorsque l'intéressé est détenu et qu'il n'y a pas d'autre raison qui rende cela impossible, et par conséquent elles ne sont pas admissibles comme preuves pour l'accusation, ni les déclarations des officiers de police qui sont intervenus dans les perquisitions comme preuves pour l'accusation.

Elle considère qu'en l'espèce, la nullité de la perquisition entraîne l'impossibilité d'affirmer légalement la découverte de la substance et des objets dont découle la condamnation pour les crimes contre la santé publique et la détention illégale d'armes, et que cette saisie ne peut être sanctionnée par le biais du témoignage des agents présents lors de la perquisition, puisque leurs témoignages respectifs sont directement liés à l'action illégale.

Cette question a été soulevée dans le précédent appel et les arguments en faveur de son rejet sont les nôtres.

Dans le cadre de cette procédure, sept perquisitions simultanées ont été effectuées et, dans cinq d'entre elles, la perquisition s'est déroulée en présence des personnes concernées dans chacune des propriétés, sauf dans deux d'entre elles, où personne n'a été trouvé et où la perquisition s'est déroulée, comme dans les autres, sous la supervision du conseiller juridique pour l'administration de la justice.

La requérante était présente lors de la perquisition à son domicile et n'aurait pas pu être présente aux autres domiciles puisque les perquisitions étaient simultanées et que, en principe, elle n'était pas résidente des autres domiciles et n'a été ni localisée ni arrêtée. Son arrestation a eu lieu précisément au moment de la perquisition.

L'article 569 de la LECrim () stipule que la perquisition d'un domicile privé s'effectue en présence de l'intéressé ou de la personne qui le représente légitimement. La jurisprudence de cette Chambre a été hésitante lorsqu'il s'est agi de préciser ce qu'il fallait entendre par "partie intéressée", puisque dans certains arrêts, il a été considéré qu'il s'agissait de la personne propriétaire du domicile en question, en tant que titulaire du droit à la vie privée affecté par l'ingérence (SSTS. 18.7.98, 16.7.2004, et 3.4.2009), tandis que d'autres arrêts ont considéré que la personne qui fait l'objet de l'enquête policière a ce caractère, dans la mesure où elle a un intérêt direct dans le résultat de la perquisition en raison des répercussions procédurales et pénales qui peuvent découler de son développement (SSTS 27.10.99, 30.1.2001 et 26.9.2006). Cette dernière position est majoritaire, de sorte que la présence de l'intéressé est requise dans la procédure, même s'il n'est pas le propriétaire du logement dans le cas où l'intéressé est détenu. Dans le STS 771/2010, du 23 septembre, suivi par de nombreux autres, il a été déclaré que la jurisprudence est certainement uniforme pour exiger la présence de la partie intéressée - la personne faisant l'objet de l'enquête - lors de la perquisition dans les cas où elle est détenue et même dans le cas où elle est différente du propriétaire du domicile ou que ce dernier est présent ou refuse d'être présent lors de la perquisition. Cette présence, si elle est possible, est requise en raison des exigences contradictoires qui doivent entourer toute procédure de preuve et, plus encore, en raison des caractéristiques des perquisitions à domicile, dans lesquelles l'absence de contradiction dans l'acte de perquisition lui-même ne peut être remplie en raison de l'activité contradictoire qui rend possible le débat du procès oral. Par conséquent, si l'intéressé est détenu, sa présence à la perquisition est obligatoire et les exceptions établies dans les paragraphes 2 et 3 de l'art. 569 LECrim ne s'appliquent pas (SSTS. 833/97 du 20.6, 40/99 du 19.1, 163/2000 du 11.2, 1944/2002 du 9.4.2003).

Cependant, dans certains cas, cette présence n'est pas possible et diverses circonstances peuvent la rendre impossible : la personne faisant l'objet de l'enquête ne peut être localisée, elle ne veut pas se présenter si elle n'est pas détenue et elle est physiquement incapable de le faire, comme c'est le cas lors de perquisitions simultanées. Dans ce dernier cas, cela a été reconnu par cette Chambre dans de nombreux arrêts, tels que les SSTS 947/2006, du 26 septembre, 771/2010, du 23 septembre et 199/2011, du 30 mars.

En l'espèce, la requérante était présente lors de la perquisition de son domicile et ne l'était pas lors des autres perquisitions, celles-ci ayant été effectuées simultanément.

Le moyen est donc rejeté et l'arrêt attaqué est confirmé dans son intégralité.

Conclusions.

En peu d'occasions, le comité de surveillance a maintenu une ligne aussi uniforme sur la question de savoir qui doit être considéré comme intéressé par une visite et une perquisition, c'est-à-dire la personne qui, indépendamment du titre formel qu'elle détient sur le domicile, peut être légalement affectée par son résultat dans le cadre du délit faisant l'objet de l'enquête. Les problèmes pratiques entre les perquisitions successives et simultanées sont également décrits, afin que la partie intéressée puisse assister à cette procédure, à moins que cela ne soit pas possible pour des raisons exceptionnelles ou en cas de force majeure.

2 - STS 358/2025, du 10 avril 2025. Informations pénales transférées en Espagne par une autorité judiciaire étrangère et poursuite de l'enquête dans notre pays avec de nouvelles enquêtes policières .²

Contexte factuel

Dans l'affaire n° 33/2021 (découlant de l'AP 25/2021 du Juzgado de Instrucción n° 3 de Talavera), suivie devant la Audiencia Provincial de Toledo, Sección 1ª, le 5 mai 2022, Evelio a été condamné en tant qu'auteur d'un crime contre la santé publique pour trafic de stupéfiants, qui contient les faits prouvés suivants : "...Suite à une communication du Ministère Public du Portugal, on a su qu'il pouvait y avoir un groupe organisé qui, depuis l'Amérique du Sud, se chargeait d'envoyer de la cocaïne en Europe, au moins en Espagne et au Portugal, et qu'il utilisait pour cela des bateaux qui faisaient escale dans le port de Porto. Depuis cette ville, la cocaïne était transportée par camion, du moins en partie, jusqu'à la ville de Talavera La Nueva, où elle était déchargée dans un entrepôt industriel portant l'étiquette Puertas Artevi. Suite à ces informations, l'Udyco a entamé une enquête qui a permis de vérifier la véracité des informations concernant l'arrivée des camions à l'entrepôt, et a donc entamé une série de surveillances et de contrôles qui ont permis de découvrir que l'entrepôt était loué par l'accusé Evelio, né en 1984, sans antécédents judiciaires, qui avait également loué un entrepôt dans la ville de Ventas de Retamosa et un local de stockage, avec le numéro, appartenant à l'entreprise Blue Space, de Leganés. Par ordonnance du 22 décembre 2020, le tribunal de première instance et d'instruction n° 3 de Talavera a autorisé l'entrée et la perquisition des entrepôts susmentionnés et du local de stockage. Sept paquets rectangulaires ont été trouvés dans le local de stockage, contenant une substance blanche, à laquelle on a appliqué le réactif approprié, qui s'est avéré positif pour la cocaïne. Après l'analyse correspondante, la substance s'est avérée être de la cocaïne, d'un poids total de six mille quatre-vingt-seize grammes et d'une richesse moyenne de 77,88 %, dont la valeur sur le marché illicite s'élèverait à la somme de deux cent trente-huit mille trois cent soixante-neuf et trente et un euros, que l'accusé possédait pour la distribuer à des tiers. Il n'a pas été prouvé que les autres accusés, Gaspar, né le NUM002 1969, sans antécédents judiciaires, et Jacinta, née en 1991, qui a été condamnée dans le jugement du 16 juin 2020 pour un délit contre la santé publique, étaient en relation avec la substance saisie..."

Base juridique

Le requérant demande l'annulation de l'ordonnance ordonnant la mise sur écoute des téléphones de la défenderesse et de l'ordonnance du 29 juillet 2020, par laquelle elle a été prorogée, ainsi que de nouvelles écoutes, demandes qui ont été formulées pour la première fois en tant que question préalable au début du procès oral et qui ont déjà été rejetées par le tribunal de première instance avec les arguments appropriés.

Le moyen, comme nous l'avons dit, coïncide avec celui soulevé en appel avec la seule différence qu'il transcrit un paragraphe du STSJ, mais avec lequel il ne discute pas, répète que la nullité des ordres susmentionnés est fondée sur le manque de motivation et

² STS 358/2025, du 10 avril 2025, publié sur le site Internet de la CGPJ par le Centre de documentation judiciaire, CENDOJ, (ROJ : STS 1628/2025 - ECLI:ES:TS:2025:1628). recours : 8375/2022. Orateur : M. Ángel Luis Hurtado Adrián.

de justification, car ils manquent d'objet et vont au-delà des dispositions contenues dans le cadre de la collaboration entre les autorités espagnoles et les autorités portugaises, et que l'irrégularité attribuée à ces ordonnances tient au fait que les personnes où la drogue devait être stockée et cachée avaient déjà été identifiées au moyen des surveillances policières effectuées les 14, 15, 17 et 19 mai, de sorte que, de l'avis de la requérante, la demande de la police d'autoriser des écoutes téléphoniques 25 jours plus tard ne repose sur aucun fondement et aucune base juridique.

Il est allégué que l'objet de la surveillance était l'arrivée du Portugal d'un camion avec une cargaison à déposer dans l'entrepôt le 14 mai 2020, et que, l'arrivée et le déchargement étant surveillés, il est logique que l'intervention policière ait été effectuée ce jour-là ou les jours suivants, et que si elle n'a pas été effectuée, c'est parce qu'il n'y a pas de certitude que les drogues sont arrivées à cet endroit. Si tel est le cas et que, 25 jours plus tard, l'écoute téléphonique est acceptée, le signataire du recours considère qu'il s'agit d'une enquête prospective, car à ce moment-là, il n'y a aucune preuve qu'un délit est en train d'être commis ou va l'être, et répète une fois de plus qu'au moment où l'ordonnance en question a été émise, il n'y avait pas de "bonne raison" ou de "forte présomption" pour justifier cette intervention, et le fait sans avancer aucun argument aux considérations que, pour rejeter une telle approche, le jugement de première instance et ensuite le jugement d'appel lui ont donné, alors qu'il réitère, une fois de plus, une demande avec des conséquences aussi traumatisantes qu'une nullité pour considérer l'enquête prospective, à laquelle il aurait dû donner beaucoup plus d'extension après l'avoir rejetée à deux reprises précédentes.

L'approche de la requérante consiste à relier l'action policière qui s'est déroulée à partir du 14, à la suite d'informations reçues des autorités portugaises, à l'enquête qui fait l'objet de la présente affaire, ce qui ressort de la lecture des faits prouvés, qui se réfère à la communication envoyée par le ministère public portugais, qui a révélé l'existence d'un groupe organisé chargé d'envoyer de la cocaïne en Europe, qui arrivait par le port de Porto et de là était transférée, au moins en partie, dans le bâtiment industriel portant le nom de Puertas Artevi dans la ville de Talavera de la Reina, loué par Evelio, autour duquel une enquête a été menée au Portugal, qui a conduit à l'émission d'un ordre d'enquête européen par le ministère public de Porto, demandant certaines procédures dans notre pays, et que, comme indiqué dans l'ordre du 22 décembre 2020, par l'ordre du 29 juin 2020, il a été convenu de reconnaître et d'exécuter. Parmi les mesures prises, il y a eu l'interception de certains téléphones, y compris celui de l'Evelio susmentionné, qui a été prolongée par l'ordonnance du 29 juillet 2020 et a été annulée par l'ordonnance du 18 septembre 2020, une enquête portugaise dans laquelle il n'y a aucune trace qu'il ait jamais été inculpé.

Les investigations policières se sont poursuivies dans notre pays, par l'intermédiaire de l'Udyco, au moyen d'une surveillance et d'un contrôle, établissant que, entre autres, l'Evelio susmentionné effectuait des mesures de sécurité, comme indiqué dans l'ordonnance, indiquant une activité criminelle présumée liée à un délit de trafic de stupéfiants, différente et postérieure à celle qui pourrait faire l'objet d'une enquête au Portugal, puisque, comme l'explique le jugement de la juridiction inférieure, "il n'existe aucune preuve que les défendeurs aient été poursuivis dans le pays voisin, de sorte que l'enquête ne pouvait se limiter à la seule identification des auteurs éventuels qui ont commis en Espagne les actes qui font l'objet d'une procédure pénale au Portugal".

En tout état de cause, l'information initiale, même si elle provenait du Portugal, a fourni des éléments qui ont justifié l'adoption des mesures prises par le juge d'instruction, y compris celle limitant les droits fondamentaux, comme l'écoute téléphonique convenue, qui ne peut donc pas être considérée comme ayant été donnée dans le cadre d'une enquête prospective, mais en même temps elle était utile pour enquêter sur l'activité criminelle présumée commise en Espagne, et soutenir le contraire, comme le soutient le M.F., est un "raisonnement difficile à soutenir, dans la mesure où le requérant semble prétendre que dans l'enquête d'un crime dont il y a connaissance préalable, il faut renoncer à enquêter sur l'existence d'autres participants possibles à un crime", est "un raisonnement difficile à soutenir, dans la mesure où le requérant semble prétendre que dans l'enquête sur un crime dont il y a connaissance préalable, il faut renoncer à enquêter sur l'existence d'autres participants possibles à un crime aussi grave qu'en l'espèce".

C'est ce qu'explique précisément l'arrêt attaqué, qui expose les raisons pour lesquelles les faits examinés au Portugal doivent être dissociés de ceux qui devaient l'être en Espagne, même si, dans les deux cas, ils étaient liés à des délits de trafic de stupéfiants, parce que l'écart entre les deux est évident et que chacun d'entre eux, en faisant nôtres les mots qui viennent d'être transcrits du M.F., aurait dû donner lieu à une enquête distincte, L'arrêt attaqué explique également cela, qui différencie les enquêtes portugaise et espagnole, lorsqu'il dit que "l'enquête ne devait pas se limiter uniquement à l'identification des personnes et du lieu où elles cachaient la drogue, car il ne s'agissait pas d'une collaboration avec les autorités portugaises pour des faits faisant l'objet d'une procédure pénale au Portugal, Il s'agissait plutôt d'informations transmises par le ministère public portugais à la police espagnole sur des faits permettant de déduire l'éventuelle commission d'un délit en Espagne, en incorporant des données objectives indiquant une activité criminelle dans notre pays, telles que l'arrivée d'un navire, le chargement de bobines, les entreprises de transport et, surtout, la destination en Espagne du matériel chargé au Portugal".

En définitive, étant donné que le juge d'instruction disposait d'indices suffisamment plausibles pour apprécier la commission présumée d'un délit de trafic de stupéfiants dans notre pays, même s'ils étaient fournis par des informations en provenance du Portugal, il n'est pas possible de parler d'une enquête prospective, car ce sont ces informations qui lui ont fourni ces éléments, en fonction desquels il a adopté les mesures d'enquête qu'il estimait appropriées, y compris la mise sur écoute du téléphone de l'une des personnes présumées impliquées, qu'il a justifiée suffisamment longuement dans son ordonnance du 29 juin 2020 et également dans l'ordonnance de prorogation du 29 juillet 2020.

Le recours est rejeté dans son intégralité et la condamnation du requérant est confirmée.

Conclusions.

La Cour de cassation évalue la portée d'un OEI envoyé officiellement par l'autorité judiciaire portugaise à l'autorité judiciaire nationale, en tant qu'instrument de coopération qui impliquait certaines mesures restreignant les droits fondamentaux. Lorsque cette ligne d'enquête n'a pas prospéré et n'a pas été menée à son terme, et qu'une procédure pénale indépendante n'a pas été suivie au Portugal pour les mêmes faits, la police judiciaire espagnole a ajouté à ces informations de nouvelles données sur les personnes faisant l'objet de l'enquête et sur d'éventuels actes criminels commis en Espagne, et a engagé une

procédure qui, sur la base des premières, a permis de démanteler un groupe criminel chargé de commettre des délits graves.

3 - STS 324/2025, section pénale 1 du 07 avril 2025. Conservation des données de communication . 3

Contexte factuel

L'Audience provinciale de Barcelone, 7e section, a prononcé la sentence n° 173/2023 du 3 mars, découlant de la procédure sommaire n° 1/2021 du tribunal d'instruction n° 1 de Sant Boi de Llobregat, suivie pour un délit contre la santé publique, qui contient entre autres les faits avérés suivants : "...il est prouvé, et il est ainsi déclaré, que depuis au moins le mois d'août 2018 les accusés Jenaro, Humberto, Fermín, Lucas et Emiliano ont formé un cadre personnel, matériel, corporatif et logistique mis au service d'un plan commun qui était de s'emparer de la cocaïne cachée dans un conteneur en provenance du Brésil qui arriverait au port de Barcelone à la mi-décembre, pour procéder à sa distribution dans cette dernière province. Jenaro était à la tête du réseau, lui fournissant une couverture financière et des contacts pour obtenir la drogue ; Humberto était chargé de la gestion et de la coordination. Fermín était chargé de la structure corporative et commerciale capable de s'emparer de la cargaison en la faisant passer pour un achat et une vente légaux de feuilles de papier Din-A4, Lucas était chargé de la logistique, en particulier de l'organisation du transport de la substance, dont Emiliano se chargerait, en la déléguant à des tiers.

En exécution de ce plan criminel, la société Campderros Salvans S.L., a acquis, par l'intermédiaire de Fermín, 1.600 boîtes de feuilles de papier DIN-A4 de la société Precisión Comercio Internacional LTDA, basée à Pinheiro-Maceió (Brésil), dont l'arrivée au port de Barcelone était prévue en décembre 2018 ; des marchandises qui ont été distribuées dans deux conteneurs de 800 boîtes de feuilles DIN-A4 chacun, conteneurs numérotés APZU3035695 et APZU3807079 affrétés à bord du navire de la compagnie maritime CMA-CGM RIO GRANDE, partant du port d'Itaguaí (Rio de Janeiro-Brésil) à destination du port de Barcelone, le 21 novembre 2018....." Le récit des faits avérés se poursuit en disant que, "...A 13h40 à la date susmentionnée, pendant le travail de chargement et de redistribution des paquets de folios dans le camion que Herminio conduisait, est tombé accidentellement du chariot élévateur mécanique employé par l'un des travailleurs de Campderros Salvans S.L., Nemesio, une boîte de papier d'aluminium sortant du conteneur portant le numéro APZU 3035695, qui, une fois brisée, a révélé plusieurs paquets rectangulaires qui se sont avérés contenir la substance stupéfiante susmentionnée. À la demande de la police, une équipe d'agents des Mossos d'Esquadra est arrivée sur les lieux et, après avoir dûment inspecté toutes les boîtes de papier d'aluminium, a trouvé à l'intérieur 1 410 paquets rectangulaires présentant les caractéristiques d'identification suivantes...".

³ STS 324/2025, section pénale 1^a du 07 avril 2025, publié sur le site du CGPJ par le Centro de Documentación Judicial, CENDOJ, (ROJ : STS 1487/2025 - ECLI:ES:TS:2025:1487). Pourvoi : 10408/2024. Orateur : M. Manuel Marchena Gómez.

Base juridique

Dans un long arrêt, la Cour suprême passe en revue les nombreuses contestations formulées par les avocats de la défense des accusés pour tenter de démontrer la justesse des condamnations, soulignant même que l'un des appelants reproche au juge d'instruction de ne pas avoir ajouté à l'ingérence que représentent les écoutes téléphoniques elles-mêmes, d'autres mesures qui renforcent l'ingérence de l'État dans le cercle d'exclusion défini par le droit au respect de la vie privée. Il est absurde d'invoquer la nullité d'un acte judiciaire d'ingérence dans la vie privée d'un suspect en reprochant au juge de ne pas avoir autorisé des restrictions encore plus sévères que celles qui ont été jugées nécessaires et proportionnées.

Rarement, comme en l'espèce, tout grief d'une éventuelle enquête prospective ou contraire aux principes de proportionnalité, de nécessité ou d'exceptionnalité - art. 588 bis a - doit nécessairement être écarté.

A partir du moment où la drogue a été découverte par hasard à la suite d'un accident lors du déchargement, le travail des Forces et Corps de Sécurité de l'Etat visant à découvrir qui avait acquis cette cargaison extraordinaire de cocaïne pour la distribuer clandestinement était pleinement justifié. Ce travail était d'ailleurs soumis au contrôle restrictif du juge d'instruction n° 1 de Sant Boi de Llobregat et à l'intervention supervisée du procureur général (art. 306 de la LECrim).

Nous passons maintenant à la contestation de la conservation des données de communication.

Le moyen incorpore une allégation concernant la demande des Mossos aux opérateurs téléphoniques de conserver les données au-delà du délai d'expiration d'un an imposé par la loi 25/2007 du 18 octobre 2007 sur la conservation des données, avec une référence marginale à l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014, qui a déclaré la nullité de la directive 2006/24/CE.

La défense fait valoir que la demande de conservation de ces données - qui n'ont pas été formellement intégrées dans le dossier - n'a pas été autorisée au préalable par le juge d'instruction.

L'arrêt attaqué reproche à la requérante de rechercher cette nullité au moyen d'une allégation générique dans laquelle il n'est pas précisé quels seraient les ordres ou les lignes interceptés". En outre, il estime que l'autorisation judiciaire est implicite dans les décisions d'habilitation qui impliquent, par leur nature même, la nécessité de conserver les données liées à ces processus de communication.

En tout état de cause, la Chambre considère qu'une telle autorisation judiciaire pour exiger des opérateurs ou de toute autre personne physique ou morale qu'ils conservent les données n'est pas obligatoire.

Cela se déduit des dispositions de art. 5 de la loi 25/2007, du 18 octobre, sur la conservation des données relatives aux communications électroniques et aux réseaux publics de communications. Cela se déduit également de art. 588 *octies* de la LECrim,

qui réglemente l'ordre préalable de conservation des données en tant que mesure de sécurité.

La première de ces dispositions s'adresse aux opérateurs qui fournissent des services de communications électroniques accessibles au public ou qui exploitent des réseaux de communications publics, selon les termes établis dans la loi 32/2003, du 3 novembre, loi générale sur les télécommunications", un critère réitéré dans art. 1 de l'actuelle loi 9/2014, du 9 mai, loi générale sur les télécommunications.

Le second - art. 588 octies de la LECrim - incorpore la même obligation de sécurité et de conservation des données lorsque le dépositaire est une personne physique ou morale et exclut explicitement la nécessité d'une autorisation judiciaire : "le ministère public ou la police judiciaire peut exiger de toute personne physique ou morale qu'elle conserve et protège des données ou des informations spécifiques incluses dans un système de stockage informatique à sa disposition jusqu'à l'obtention de l'autorisation judiciaire correspondante pour leur transfert conformément aux dispositions des articles précédents".

Par conséquent, tant le procureur que les forces et corps de sécurité de l'État sont habilités à émettre, sans qu'une autorisation judiciaire soit nécessaire, une telle ordonnance de conservation qui, logiquement, n'a de sens que dans le cadre d'une enquête dans laquelle la nécessité ultérieure d'intégrer ces données dans la procédure pénale engagée est prévisible.

L'absence d'exigence d'une autorisation judiciaire ressort non seulement de la formulation de ce précepte, mais aussi de l'exposé des motifs de LO 13/2015, du 5 octobre, qui a introduit l'article 588 octies, en précisant que, enfin, et en ce qui concerne les procédures d'investigation technologique, la réforme envisage comme mesure de sécurité l'ordonnance de conservation des données, dont l'objet est de garantir la conservation de données spécifiques et d'informations de toute nature qui sont stockées dans un système informatique jusqu'à l'obtention de l'autorisation judiciaire correspondante.

Conclusions

Ce STS fait clairement la distinction entre une mesure de conservation des données et d'autres mesures technologiques, en distinguant les cas où une autorisation judiciaire est nécessaire et ceux où le FCSE peut agir directement. Les mesures technologiques prévues aux articles 588 bis et suivants de la LECrim, qui dans certains cas n'ont pas été mises à jour, telles que l'utilisation de drones, l'utilisation de l'IA...

4 - STS 294/2025, du 28 mars 2025. Champ d'application du principe d'insignifiance et de toxicité dans les crimes contre la santé publique .4

Contexte factuel.

Le tribunal d'instruction n° 11 de Palma de Majorque a ouvert la procédure préliminaire n° 649/2020, qui a été transmise au tribunal pénal n° 2 de Palma de Majorque, pour être jugée dans le cadre de la procédure abrégée n° 11/2022, qui a dicté la sentence n° 111/2022, datée du 28 mars 2022, qui contient les faits prouvés suivants : "...SOUS-ANCIENS. Il est prouvé et déclaré que l'accusé Lázaro, majeur, sans antécédents judiciaires et privé de liberté pour cette cause le 9 juillet 2020, vers 00h15, le 9 juillet 2020, vers 00h15, le 9 juillet 2020 :15 heures le 9 juillet 2020, il se trouvait dans la rue General García Ruiz à Magalluf, contactant un touriste britannique à qui il a offert de la cocaïne en échange de 50€, lui remettant un emballage avec ladite substance, recevant le montant de 50€, un fait qui a été observé par une force de police locale de Calviá qui a arrêté son véhicule et s'est rendu à l'endroit où le sujet britannique s'était rendu avec un ami, Ils les ont trouvés assis en train de renifler la substance et leur ont dit qu'ils venaient d'acheter de la cocaïne à un jeune homme de couleur et qu'ils avaient payé 50€, en essayant de cacher avec leurs pieds la cocaïne qui restait dans l'emballage. Ils sont ensuite partis dans la direction opposée et ont procédé à l'interception de Lázaro, interceptant 50€ dans son portefeuille et 50€ de plus dans le tissu de son pantalon où il portait un cordon en guise de ceinture. La substance restée dans l'emballage, une fois analysée, s'est avérée être de la cocaïne d'une pureté de 19,15 % et d'une valeur au détail de 4,83 €..."

Le jugement du tribunal pénal a fait l'objet d'un appel devant l'Audiencia Provincial, qui a rejeté l'appel. La Cour Suprême a confirmé l'appel et a rendu un jugement d'acquiescement.

Base juridique.

La jurisprudence admet le caractère atypique de la conduite de trafic lorsque, en raison de son insignifiance absolue, la substance ne constitue plus, par ses effets, une drogue toxique ou un stupéfiant, mais un produit inoffensif en raison de sa toxicité précaire (SSTS 527/1998, du 15 avril ; 985/1998, du 20 juillet ; 789/99, du 14 avril ; 1453/2001, du 16 juillet ; 1081/2003, du 21 juillet ; et 14/2005, du 12 février). Le principe de l'insignifiance justifierait l'impunité lorsque la quantité de drogue est si faible qu'elle est incapable de produire un quelconque effet nocif sur la santé. Il y a absence d'illégalité matérielle en raison de l'absence de risque réel pour le droit protégé (SSTS 1441/2000, 22 septembre ; 1889/2000, 11 décembre ; 1591/2001, 10 décembre ; 1439/2001, 18 juillet ; et 216/2002, 11 mai).

En revanche, il convient de souligner que notre jurisprudence la plus récente a nuancé l'utilisation du terme "insignifiance", préférant parler de "toxicité". Ne tombe pas sous le coup de l'infraction la transmission de substances qui, en raison de leur absence de nocivité, n'entraîneraient pas de risque.

⁴ STS 294/2025, section pénale 1^a du 28 mars 2025, publié sur le site du CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ : STS 1335/2025 - ECLI:ES:TS:2025:1335), recours : 6755/2022. Intervenante : Mme Susana Polo García.

Cette doctrine doit être appliquée de manière exceptionnelle et restrictive, mais avec certitude. Dans ce contexte, cette Chambre continue de fonctionner selon les critères établis lors de la session plénière du 24 janvier 2003. Ceci est confirmé par de nombreux précédents (SSTS 936/2007, du 21 novembre ; 1110/2007, du 19 décembre ; 183/2008, du 29 avril ; et 1168/2009, du 16 novembre) (voir STS 587/2017, du 20 juillet).

En ce qui concerne le concept de minimum psychoactif et ses répercussions pénales dans l'élément subjectif du délit, STS 1982/2002, du 28 janvier 2004, nous dit que les minimums psychoactifs sont les paramètres proposés par un organisme officiel à la solvabilité scientifique reconnue, tel que l'Institut national de toxicologie, qui supposent un degré d'affectation du système nerveux central, déterminant une série d'effets sur la santé des personnes, Il s'agit bien sûr de produits nocifs, car ils présentent un niveau minimum de toxicité, mais aussi une composante addictive, ce qui signifie que l'absence de consommation conduit à la compulsion. Il s'agit donc de drogues qui portent atteinte à la santé publique, entendue comme la santé des membres individuels de la communauté, et dont les sanctions sont conçues par le législateur pénal, en fonction de la gravité ou non de l'atteinte. Ces minima supposent que la quantité transmise est un type de stupéfiant, de toxique ou de substance psychotrope figurant dans les conventions internationales en la matière, au moyen des listes prévues à cet effet. Ils répondent donc à la nature objective de l'infraction et affectent l'illégalité tant formelle que matérielle. Ces minima ont été proposés par le rapport de l'Institut National de Toxicologie, et dans les marges permises par cette expertise, ils peuvent être interprétés, sans nécessairement nécessiter un automatisme judiciaire (STS 580/2017, du 20 juillet).

En d'autres termes, toute substance stupéfiante qui dépasse la dose psychoactive minimale, génère les dommages à la santé que la règle typique sanctionne et, par conséquent, si elle est gravement nuisible à la santé en raison de sa nature et de sa classification, elle continue à l'être, quelle que soit la quantité et la pureté (ou le degré d'adultération, si l'on préfère), une fois que la dose psychoactive minimale a été dépassée (STS 723/2017, 7 novembre).

Quoi qu'il en soit, sur cette question, nous devons nous rappeler notre doctrine jurisprudentielle, qui trouve son origine dans la séance plénière non juridictionnelle du 24 janvier 2003 qui, en ce qui concerne la cocaïne, a établi que son principe actif opère à partir de 50 milligrammes (0,05 gramme) ; Ce critère a été accepté par la Chambre et repris lors de la session plénière non juridictionnelle du 3 février 2005, au cours de laquelle il a été convenu de "maintenir le critère de l'Institut national de toxicologie concernant les doses psychoactives minimales, jusqu'à ce qu'une réforme juridique soit élaborée ou qu'un autre critère ou une autre solution soit adopté".

En effet, comme le souligne le requérant, le compte rendu des faits n'inclut pas la quantité de cocaïne saisie, de plus, selon le rapport du département de la santé de la délégation du gouvernement des îles Baléares, la substance saisie par la police était de 0,093 gramme de cocaïne. Par conséquent, si, comme l'indiquent les faits prouvés, la pureté est de 19,15 %, nous avons un total de 0,017 gramme de cocaïne nette, soit 17 milligrammes, ce qui est nettement inférieur aux 50 milligrammes au-delà desquels il y a un risque pour la santé publique.

S'il est vrai que le récit des faits relate de manière incomplète un événement qui pourrait constituer, dans son ensemble, un acte de trafic, le fait est qu'en définitive seule

l'occupation par l'acheteur présumé - non identifié, bien que la police dise lui avoir parlé - d'une quantité infinitésimale de drogue, 0,093 grammes, d'une pureté de 19,15 %, est déclarée prouvée, donc, Nous nous trouvons donc avec un total de 0,017 grammes de cocaïne nette -17 milligrammes-, une quantité inférieure à la dose psychoactive minimale, sans considérer expressément que l'occupation d'autres substances narcotiques par l'accusé est accréditée, de sorte qu'on ne peut pas raisonnablement déduire, à partir de cette quantité minimale, qu'il a été impliqué dans le trafic et, surtout, il faut considérer qu'il n'a pas de pertinence pénale en raison de son caractère inoffensif pour la santé publique.

Conclusions.

Malgré la clarté de l'exposé des faits avérés, un acte de trafic de drogue au détail dans lequel le rôle de l'acheteur et du vendeur est détaillé, cette STS n'apporte rien de nouveau à la ligne jurisprudentielle déjà suivie depuis des années et qui reste inchangée, sur le principe de l'insignifiance qui se prolonge désormais avec le qualificatif de toxicité, lorsqu'il s'agit d'appliquer le critère de l'INTCF sur les doses psychoactives minimales pour apprécier le caractère délictueux de l'infraction.

5 - SAN 8/2025 du 2 avril 2025. Délit de destruction terroriste . 5

Contexte factuel.

La présente procédure judiciaire a été engagée à la suite d'une communication par fax du secrétaire d'État à l'intérieur, TEPOL, informant de l'explosion d'un engin explosif contrôlé à l'aéroport "El Altet" d'Alicante. Le tribunal central d'instruction numéro 2 de Madrid a rendu une ordonnance d'ouverture de la procédure préliminaire le 31 juillet 1995 et, après l'enquête correspondante, un acte d'accusation a été délivré le 19 mai 2010 à l'encontre de Melisa pour les délits de destruction terroriste dans le degré de frustration.

Base juridique.

Cet arrêt de l'Audiencia Nacional indique que, dans le dossier de la procédure, on trouve, en premier lieu, un rapport de la direction générale de la Garde civile de Guipúzcoa du 10 mai 2001, folio 294 et suivants du volume I de la procédure, qui informe l'Audiencia Nacional que la prévenue, dans une autre procédure (26/01), reconnaît aussi expressément avoir placé l'engin à l'aéroport d'Alicante, dans laquelle il est indiqué à la chambre centrale d'instruction que la prévenue, dans le cadre d'une autre procédure (26/01), également du même commandement, reconnaît expressément avoir placé le dispositif à l'aéroport d'Alicante avec une autre personne (qui n'est pas jugée) à l'intérieur d'un sac et d'une corbeille à papier. Ces déclarations sont contenues dans sa deuxième déclaration faite à la Guardia Civil le 31 mars 2001 (folio 163 du volume I de la procédure), indiquant également que c'est le même jour qu'il a placé un autre dispositif dans l'office de tourisme de Denia.....

Lors du procès, et après un travail louable de la Garde civile, il existe un vide probatoire incompréhensible que les membres de la Cour dénoncent eux-mêmes et qui se

⁵ SAN 8/2025, section pénale 3^a du 02 avril 2025, publiée sur le site web du CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ : SAN 1662/2025 - ECLI:ES:AN:2025:1662). Pourvoi : 132/2010. Orateur : M. Jesús Eduardo Gutiérrez Gómez.

lit comme suit : "...Nonobstant ce qui précède, et malgré les efforts déployés par le ministère public, nous comprenons qu'il existe un vide probatoire important qui nous oblige à prononcer l'acquittement de l'accusée". Un vide probatoire qui découle du manque et de l'absence de preuve d'une information transcendante, telle que la paternité de la lettre manuscrite que le ministère public attribue à Melisa, et pour laquelle aucune preuve n'a été produite. Ce vide probatoire est dû à la défaillance des policiers qui ont émis le rapport d'expertise graphologique, inclus dans la procédure dans ce que l'on appelle l'"Annexe de documentation", et où sont analysés en détail les documents trouvés en France, y compris la "kantada" attribuée à l'accusée. Ce rapport d'expertise graphologique daté du 20 mai 2008 et rédigé par des officiers de police ayant les numéros de licence professionnelle NUM005 et NUM006, a été ratifié dans la phase d'enquête devant la Cour d'instruction centrale, mais par la suite le ministère public ne les a pas proposés comme preuves d'expertise, et par conséquent, comme ils n'ont pas été "apportés" au procès, et n'ayant pas été soumis à la contradiction entre les parties, il ne peut être retenu comme preuve contre la défenderesse, ayant été expressément contesté par sa défense, défenderesse qui, par ailleurs, en séance plénière a déclaré de manière claire et patente qu'elle ne reconnaissait pas le document en question comme étant le sien et qu'elle ne l'avait pas écrit. D'autre part, le rapport 7/2015, un rapport que l'on pourrait qualifier de "rapport d'intelligence" qui analyse l'existence et les composantes du commando de l'ETA connu sous le nom d'Ibarla, son activité et les données sur les attentats commis par ce commando terroriste, et sa comparaison avec les documents trouvés en France, Ce rapport, qui aurait pu éclairer la possible paternité de la pose de l'explosif à l'aéroport d'Alicante, contrairement à la négation des faits par l'accusé, n'a pas non plus fait l'objet de preuves en séance plénière, les auteurs du rapport n'ayant pas été proposés en tant qu'experts. Par conséquent, les déclarations des témoins qui ont comparu au procès n'ont aucune valeur probante en tant que preuve pour l'accusation et en tant que preuve de la paternité de l'accusé, puisqu'il a été injustement "présumé" et supposé que la "kantada" était la seule preuve solide pour l'accusation (la déclaration de l'accusé), (la déclaration de la police n'a aucune valeur en tant que preuve pour l'accusation car elle n'a pas été vérifiée ou ratifiée par l'accusé devant la Cour centrale d'enquête préliminaire) avait été rédigée par l'accusé, de sorte que la preuve des éventuelles divergences entre ce document et la déclaration de la police ne nous est guère utile, car l'exigence ou la condition préalable, selon laquelle la paternité de ce document a été accréditée, n'est pas remplie.

Par conséquent, et sans apprécier les autres éléments de preuve, l'accusé doit être acquitté avec toutes les conditions nécessaires à l'acquittement..."

Conclusions.

Un témoignage saignant que ce SAN n°8/2025 Section 3 reprend, alors que le travail policier est impeccable et que le travail dans la phase préliminaire est plus que complet. Le ministère public a commis une grave erreur en ne proposant pas en séance plénière le témoignage des agents qui ont analysé la documentation de l'accusé et des auteurs du rapport de l'expert en intelligence. Il n'y avait pas d'autre option que l'acquittement.

6 - STS 308/2025, du 2 avril 2025. Enquête policière en Espagne découlant de la connaissance d'un OEB délivré par les autorités judiciaires d'un autre pays pour une autre infraction pénale. Présence des détenus lors d'une perquisition à domicile
 ـ6

Contexte factuel.

Le tribunal d'instruction n° 1 de Coín a ouvert une procédure abrégée 22/2022 pour délits contre la santé publique et détention illégale d'armes contre, entre autres, Clemente, David et Eliseo, qui, une fois conclue, a été renvoyée pour jugement à l'Audience provinciale de Malaga, 3ème section. Après avoir engagé la procédure abrégée 54/2022, elle a rendu, le 23 novembre 2022, le jugement n° 362/22, qui contient, entre autres, les faits avérés suivants : "...Il est avéré et déclaré que les autorités policières de Malaga savaient que Clemente, majeur, sans antécédents judiciaires, de nationalité britannique et faisant l'objet d'un mandat d'arrêt international émis par les autorités du Royaume-Uni, pouvait résider dans cette province, plus précisément quelque part dans la vallée du Guadalhorce ou à Coín. Après avoir mené les enquêtes nécessaires, les enquêteurs ont conclu qu'il pourrait résider à l'adresse xxx dans la ville de Coín. C'est pourquoi une surveillance policière a été effectuée les 3, 4 et 5 mai 2022, dans la propriété susmentionnée à l'adresse xxx à Coín, où les policiers ont finalement appris avec certitude que Clemente vivait avec d'autres hommes. Plus précisément, les jours indiqués, Clemente, majeur et sans casier judiciaire, David et Eliseo, tous majeurs et sans casier judiciaire, et Fidel, majeur et sans casier judiciaire, qui est entré dans la propriété susmentionnée à un moment donné entre la nuit du 3 mai, lorsqu'il a été libéré de prison, et le 5 mai à 20 h 35, lorsqu'il a été vu en train de quitter la propriété pour se rendre dans un centre sportif, se trouvaient à l'intérieur de la propriété. Parmi eux, c'est David et Eliseo qui ont quitté la propriété pour faire les achats nécessaires, et ils l'ont fait à bord d'un véhicule Volkswagen polo avec des plaques d'immatriculation anglaises, en adoptant des mesures de sécurité au volant pour vérifier s'ils étaient suivis, comme faire plusieurs fois le tour des ronds-points ou ne pas garer le véhicule à la porte de la propriété, mais à proximité de la maison.

Le 5 mai vers 20 h 35, Clemente, Fidel, David et Eliseo sont sortis ensemble de la maison, Fidel fermant la porte de la maison, qui portait alors un sac à dos noir sur le dos, qu'il a remis à Clemente en chemin. Les quatre personnes susmentionnées se sont rendues au BlueLife Sportclub and Spa Gymnasium, situé dans le centre commercial La Trocha à Coín, où les policiers sont intervenus pour arrêter les quatre hommes susmentionnés. Au moment de l'arrestation, le sac à dos noir que Fidel portait sur le dos à la sortie de la maison a été déposé aux pieds de Fidel et de Clemente. À l'intérieur du sac à dos, après inspection, on a trouvé un pistolet Ruger P89 de calibre 9 mm Parabellum, modèle P89, avec munitions et sans cran de sûreté, dont le numéro de série avait été enlevé. Après l'analyse pertinente, il était dans un état de conservation correct et son fonctionnement mécanique et opérationnel était également correct, tant en simple qu'en double action, et il pouvait être utilisé. Ni Fidel, ni Clemente, ni David, ni Eliseo n'étaient en possession d'une licence pour cette arme.

⁶ STS 308/2025, section pénale 1ª du 02 avril 2025, publié sur le site du CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ : STS 1482/2025 - ECLI:ES:TS:2025:1482), recours : 11312/2023. Orateur : M. Pablo Llarena Conde.

Le 6 mai 2022, le tribunal de Coín a rendu une ordonnance autorisant l'entrée et la perquisition de la maison sise à l'adresse xxx à Coín par ordonnance du 6 mai 2022, dans laquelle une grande quantité de stupéfiants a été trouvée...".

Base juridique

Il est surprenant que la défense des accusés n'ait pas soulevé l'éventuelle nullité des actions menées par la police judiciaire, lorsque, connaissant l'existence d'un mandat d'arrêt européen, elle a ouvert une enquête et n'a pas procédé à l'arrestation immédiate de la personne recherchée. Rien n'est dit dans le jugement, et c'est tant mieux, car il entérine tout le travail policier, qui est immédiatement rapporté au juge d'instruction, qui accepte même l'entrée et la perquisition du domicile pour l'acte effectué en Espagne. Comme nous le verrons, le jugement de l'Audiencia Provincial de Malaga a été condamnatore et le Tribunal Suprême a rejeté le pourvoi en cassation.

C'est l'information de l'affaire qui est transférée au tribunal de Coín et que nous voyons souvent dans la pratique, par exemple, l'existence non seulement d'OEDE mais aussi de perquisitions et de saisies au niveau national, ce qui nous amènerait à penser qu'il y a un besoin immédiat d'arrestation alors que ce n'est pas toujours le cas, comme nous le voyons dans cette STS.

Les requérants soutiennent que la procédure de perquisition et d'entrée effectuée le 6 mai 2022 dans la maison située à l'adresse xxx dans la ville de Coín est nulle et non avenue parce que, s'agissant de la résidence habituelle des quatre prévenus et que tous étaient en état d'arrestation, les officiers de police n'ont pris que Fidel pour témoin lors de la perquisition. Ils considèrent donc que les résultats de cette enquête sont nuls et non avendus et qu'ils ne peuvent être utilisés comme preuves légitimes à charge, et qu'ils doivent être acquittés parce qu'il n'y a pas d'autres preuves permettant d'établir la responsabilité des appelants.

Dans les arrêts rendus par cette chambre 420/2014, du 2 juin, ou 508/2015, du 27 juillet (affaire Malaya), citant d'autres précédents, nous avons résumé notre doctrine sur l'exigence de la présence de l'intéressé dans la pratique de l'entrée et de la perquisition du domicile.

Nous y avons dit que le fondement de l'exigence de la présence de l'intéressé ou de son représentant lors de l'entrée et de la perquisition du domicile ordonnées par l'autorité judiciaire dans le cadre d'une procédure pénale réside, en premier lieu, dans le fait que cette procédure affecte un droit personnel, de nature constitutionnelle, qui est le droit à l'intimité de la personne, puisque le domicile constitutionnellement protégé, en tant que logement ou habitation d'une personne, est étroitement lié à sa sphère d'intimité, puisque ce qui est protégé n'est pas seulement un espace physique mais aussi l'émanation d'une personne physique et de sa sphère privée (STC 188/2013, du 4 novembre, en relation avec art. 18 2e CE et art. 8 CEDH). Deuxièmement, cela affecte le droit à un procès équitable, parce que le résultat de cette procédure constituera une preuve dans le procès contre l'accusé dont il a été convenu de perquisitionner le domicile, ce qui détermine que dans la pratique de la perquisition la contradiction est garantie afin d'assurer la validité de la perquisition en tant que preuve préconstituée.

Le droit procédural prévoit donc, comme condition pour la pratique de la recherche, la présence de l'intéressé ou de la personne qui le représente légalement (art. 569 LECrim). Et l'intéressé visé à l'article 569 de la LECrim n'est pas nécessairement le propriétaire, au sens de propriétaire ou de locataire du bien. Ce qui est déterminant, ce n'est pas l'identité du propriétaire, qui peut être inconnu, ne pas résider dans le logement, ou même être une personne morale, mais l'identité du résident du logement, car c'est sa vie privée qui va être affectée.

En règle générale, la personne intéressée par la perquisition est le défendeur, car le résultat de la perquisition aura une incidence sur sa défense, même si ce n'est pas nécessairement le défendeur qui est présent lors de la perquisition légalement autorisée. L'accusé ou la personne contre laquelle la procédure est dirigée peut être introuvable ou simplement hors du domicile et introuvable au moment de la perquisition. L'entrée et la perquisition d'un domicile autorisées dans le cadre d'une procédure judiciaire pour une infraction pénale est, par nature, une procédure urgente qui ne peut être retardée en attendant que l'accusé rentre chez lui ou qu'il soit localisé par la police. Pour cette raison, la loi autorise à se passer de l'intéressé "lorsqu'il n'est pas présent", ce qui fait clairement référence à l'accusé, et dans ces cas la perquisition peut être effectuée en présence de n'importe lequel de ses parents majeurs, la doctrine jurisprudentielle considérant, compte tenu d'une réalité sociale où le regroupement des habitations ne se fait plus nécessairement par familles au sens strict, que cette règle est applicable à tous les habitants de l'habitation, majeurs, même s'ils ne sont pas parents au sens strict du terme.

En revanche, la présence de l'accusé lors de la perquisition est requise lorsqu'il est détenu ou placé en garde à vue ou en détention judiciaire, car dans ces cas, il n'est pas justifié de porter atteinte à son droit à la contradiction, qui est mieux garanti par la présence effective de l'accusé lors de la perquisition.

En tout état de cause, nous avons également rappelé dans ces arrêts que cette règle n'est pas applicable aux cas de force majeure, dans lesquels l'absence de l'accusé, bien qu'il soit à la disposition de la police, est justifiée. Nous avons cité comme exemple les cas d'hospitalisation de l'accusé, ou d'arrestation dans un lieu éloigné du domicile, ou dans le cas de perquisitions effectuées simultanément dans plusieurs domiciles. Et aussi lorsque l'impossibilité de leur présence est de nature juridique, par exemple lorsque l'enquête a été déclarée secrète (STS 143/2013, 28 février).

Et lorsqu'il y a plusieurs résidents dans la résidence, dans nos SSTS 336/2017, du 11 mai ou 913/2023, du 13 décembre, rappelant les SSTS 698/2002, du 17 avril, 1108/2005, du 22 septembre, 352/2006, du 15 mars, 684/2014, du 2 octobre ou 79/2015, du 13 février, nous soulignons que la validité et l'efficacité de la procédure d'entrée et de perquisition ne sont pas affectées par la présence de l'un des résidents, à condition que celui-ci n'ait pas d'intérêts contraires à ceux des autres prévenus. Sans préjudice du fait que, dans ces cas, malgré la validité de la perquisition et afin de garantir le respect du droit à la contradiction, qui fait partie du droit de défense le plus large, la perquisition ne peut pas être considérée comme une preuve préconstituée et il sera nécessaire que, au-delà de la simple lecture du procès-verbal rédigé pendant son exécution, les témoins qui ont approché ou assisté à sa pratique comparaissent pour témoigner dans le procès oral.

Les moyens sont donc rejetés.

Sans préjudice du fait qu'en l'espèce, la conduite et la garde de toutes les personnes privées de liberté auraient affecté la disponibilité du personnel policier affecté à la petite ville où les requérants exerçaient leurs activités criminelles et où ils étaient détenus, puisqu'un grand nombre d'agents auraient été nécessaires pour le transfert et la surveillance des quatre prévenus et pour la conduite de l'enquête, une analyse objective des circonstances concomitantes a permis aux enquêteurs de fonder l'absence de contradiction d'intérêts entre les personnes faisant l'objet de l'enquête. En particulier, le système de surveillance policière, mis en place pendant trois jours pour surveiller les habitants de la maison pendant une longue période, a permis d'établir qu'ils étaient tous résidents de la maison et qu'ils agissaient tous de concert. En particulier, David et Eliseo, lorsqu'ils quittaient la maison en voiture, prenaient des mesures de sécurité pour vérifier s'ils étaient suivis. De plus, eux et les autres détenus ont parfois agi de concert et ont même échangé des objets tels qu'un sac à dos. Et cette absence présumée d'intérêts contradictoires a été confirmée par les quantités importantes de stupéfiants saisis ainsi que par le nombre et l'emplacement des armes saisies, puisque les témoignages, qui ont été contredits en séance plénière, montrent que les drogues étaient visibles par tous les habitants de la maison et n'étaient pas cachées dans une pièce destinée à l'usage exclusif de l'un d'entre eux, ce qui exclut la possibilité qu'un responsable tente de se défaire sur les autres habitants de sa seule responsabilité. C'est ainsi que les trois pistolets ont également été saisis, ce qui a conduit à leur condamnation en tant qu'auteurs du délit de détention illégale d'armes.

Conclusions.

Après avoir approuvé l'enquête dans une affaire qui était basée sur la connaissance policière d'un OEB émis par les autorités judiciaires du Royaume-Uni pour un acte criminel différent, et sans que la défense n'ait contesté la possible omission du devoir de poursuivre les crimes par le FCSE en n'arrêtant pas immédiatement la personne couverte par l'OEB en vigueur, et en évitant ainsi l'enquête ouverte devant le Tribunal de Coín, le présent STS 308/2025 décrit de manière phénoménale et didactique qui bénéficie du concept de partie intéressée dans le cadre d'une entrée et d'une perquisition dans un domicile, que la personne soit détenue ou non, en établissant une règle générale et des exceptions dans des cas extraordinaires. Il délimite également les conflits d'intérêts possibles entre les personnes concernées.

7- STS 295/2025, section pénale 1^a du 28 mars 2025, crime de harcèlement, "stalking".⁷

Contexte factuel.

Le Tribunal de la violence à l'égard des femmes n° 1 de Medio Cudeyo a ouvert la procédure d'urgence n° 36/2021, qui a été transmise au tribunal pénal n° 5 de Santander, pour être jugée dans le cadre de la procédure accélérée n° 125/2021, qui a rendu la sentence n° 285/2021, datée du 25 novembre 2021, qui contient les faits prouvés suivants : "... Il a été prouvé que l'accusé Basilio, majeur et sans antécédents judiciaires calculables aux fins de récidive, qui a entretenu une relation sentimentale pendant un an avec

⁷ STS 295/2025, article pénal 1^a du 28 mars 2025, delito de acoso, "stalking", publié sur le site du CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ : STS 1348/2025 - ECLI:ES:TS:2025:1348), recours : 7251/2022. Intervenante : Mme Susana Polo García.

Concepción, domiciliée à Iruz (Santiurde de Toranzo), qui a pris fin en juillet 2020, l'a appelée au téléphone depuis le mois d'octobre de la même année, a envoyé des messages WhatsApp et des lettres avec insistance, lui demandant pardon et lui demandant de reprendre la relation, en disant "ma vie n'a pas de sens, que je pensais à la meilleure façon de disparaître, qu'est-ce que je vais faire maintenant, que la vie n'a pas de sens pour moi", ayant été trouvé à 09h00 le 15 décembre. Le 15 décembre à 9 heures, il a été trouvé assis sur une chaise dans son jardin, à moitié inconscient, les yeux révulsés, et a dû être évacué à l'hôpital. Le 1er janvier 2021, il s'est présenté à son domicile en frappant à la porte, puis il l'a constamment appelé et lui a envoyé une lettre par mois, tout cela dans l'intention de modifier sérieusement sa vie, bien qu'il sache que Concepción ne veut entretenir aucun type de relation avec lui...".

La troisième section de l'Audience provinciale de Santander a fait droit à l'appel du condamné et l'a acquitté, et le représentant de la victime a formé un pourvoi en cassation, qui a été confirmé, condamnant à nouveau l'accusé.

Base juridique.

Étant donné le caractère frappant des décisions judiciaires, condamnation en première instance, acquittement en appel et nouvelle condamnation en appel, la jurisprudence de la Cour européenne des droits de l'homme permet le réexamen des acquittements lorsque la Cour suprême agit dans les limites de la violation de la loi, en examinant des questions purement juridiques. En d'autres termes, lorsque cette chambre se limite à corriger les erreurs de présomption et à établir des critères d'interprétation uniformes pour garantir la sécurité juridique, la prévisibilité des décisions judiciaires, l'égalité des citoyens devant la loi pénale et l'unité du système pénal et de la procédure pénale, sans modifier aucune hypothèse factuelle.

L'article 172.3 du Code pénal, en vigueur au moment de la commission des faits - le précepte ayant été réformé par la LO 1/2023 du 28 février - punit expressément quiconque "harcèle une personne en accomplissant de manière insistante et répétée, sans y être légitimement autorisé, l'un des comportements suivants et, de cette manière, altère gravement le déroulement de sa vie quotidienne". L'article susmentionné, qui définit le délit de harcèlement, a été introduit dans le Code pénal par la L.O. 1/2015 du 30 mars 2015. L'article 1/2015, du 30 mars, dont l'exposé des motifs précise qu'il concerne "tous les cas où, sans nécessairement impliquer l'annonce explicite ou non de l'intention de nuire (menaces) ou l'utilisation directe de la violence pour restreindre la liberté de la victime (contrainte), il y a des comportements répétés par lesquels la liberté et le sentiment de sécurité de la victime sont gravement compromis, qui est soumise à une persécution ou à une surveillance constante, à des appels répétés ou à d'autres actes continus de harcèlement".

C'est en ces termes que la jurisprudence s'est prononcée depuis l'arrêt de la plénière 324/2017, du 8 mai, et 554/2017, du 12 juillet, ce dernier en référence expresse au précédent, où il est affirmé, entre autres, que, par conséquent, on peut affirmer que de manière insistante et répétée, cela équivaut à dire qu'il y a une répétition d'actions de même nature - un continuum - qui se répète dans le temps, dans une période non spécifiée dans le type, on peut affirmer que de manière insistante et réitérative, cela revient à dire que l'on se trouve face à une réitération d'actions de même nature - un continuum - qui se répète dans le temps, dans une période non précisée dans le type criminel, et que l'on est

en présence d'un type criminel très "attaché" aux profils et aux circonstances spécifiques de l'affaire poursuivie. En d'autres termes, l'analyse de chaque cas spécifique, compte tenu des actions menées par l'agent avec insistance et répétition, et d'autre part, compte tenu de l'aptitude de ces actions à altérer gravement la vie et la tranquillité de la victime, nous conduira à l'existence ou non d'un tel crime de harcèlement, et il appartient à cette Cour de cassation, étant donné que le recours est basé sur la double instance - sentence du tribunal pénal et sentence d'appel dictée par l'Audience provinciale - de déterminer si, compte tenu des faits prouvés, les éléments qui forment l'épine dorsale du crime existent ou non.

D'autre part, outre la définition juridique, il existe des définitions du phénomène dans la communauté scientifique, essentiellement dans le domaine de la psychologie et de la psychiatrie, qui, en règle générale, le définissent comme des comportements qu'un individu inflige à un autre au moyen d'intrusions ou de communications non désirées, identifiant l'intrusion au fait de persécuter, rôder, planer, surveiller, approcher, et communiquer avec des comportements tels que l'envoi de lettres, d'appels téléphoniques, de courriers électroniques, de graffitis ou de notes sur la voiture, ou des comportements associés tels que la commande de services au nom de la victime, les fausses accusations, etc.

L'article 172 ter décrit l'infraction pénale en termes généraux, en utilisant le verbe "harceler", un terme dont la définition ne fait pas l'objet d'un consensus dans notre système juridique, en particulier en ce qui concerne la nécessité d'autant d'actes que nécessaire, mais nous ne pouvons ignorer le fait que le harcèlement sexuel et le harcèlement fondé sur le sexe ne nécessitent pas de répétition ou de persistance, conformément au concept de ce dernier dans art. 7.1 et 7.2. Les articles 7.1 et 7.2 de la loi organique 3/2007, du 22 mars, pour l'égalité effective des femmes et des hommes, et l'introduction dans notre droit pénal du délit de stalking, constituent une réponse supplémentaire à la lutte contre la violence de genre et au respect des normes internationales et plus particulièrement de la Convention d'Istanbul.

En ce qui concerne l'altération grave de la vie quotidienne, nous avons dit que le délit ne requiert pas de planification, mais une séquence méthodique d'actions qui obligent la victime, comme seule issue, à changer ses habitudes quotidiennes. Pour évaluer l'aptitude de l'action séquentielle à modifier les habitudes quotidiennes de la victime, il faut prendre en compte la norme de "l'homme moyen", bien que celle-ci soit nuancée par les circonstances spécifiques de la victime (vulnérabilité, fragilité psychologique, etc.) qui ne peuvent être totalement ignorées (STS 639/2022, du 23 juin).

Nous nous attendons à ce que l'appel soit accueilli, avec pour conséquence l'annulation de l'acquittement et son remplacement par une condamnation.

L'exposé des faits avérés décrit le comportement de l'accusé qui, pendant une période d'au moins trois mois, a téléphoné à plusieurs reprises à son ex-partenaire, lui a envoyé des messages WhatsApp et des lettres, avec insistance selon l'exposé, dans tous les cas en demandant pardon et en demandant à son ex-partenaire de reprendre la relation qui avait cessé depuis des mois, en disant "ma vie n'a pas de sens, que je réfléchissais à la meilleure façon de disparaître, qu'est-ce que je vais faire maintenant, que la vie n'a pas de sens pour moi", un jour, la victime l'a même trouvé assis sur une chaise dans son jardin "à moitié inconscient, les yeux révulsés et il a dû être évacué à l'hôpital", se rendant 15

jours plus tard au domicile de Concepción, frappant à la porte, puis lui téléphonant sans cesse à nouveau et lui envoyant une lettre par mois, avec l'intention susmentionnée de reprendre la relation tout en sachant que Concepción ne voulait entretenir aucun type de relation avec lui.

Le délit de harcèlement protège la liberté individuelle et le droit de vivre une vie paisible et sans angoisse. Les messages, l'apparition au domicile de la victime montrant sa tentative de suicide afin de la rendre responsable, ainsi que les appels et les messages envoyés, sont en eux-mêmes susceptibles de perturber les habitudes, les coutumes, les routines ou le mode de vie de toute personne, en tenant compte de la norme de "l'homme/femme moyen", le tribunal pénal reflétant dans son raisonnement que ce qui précède a obligé la victime à recevoir un soutien psychologique, un fait qui ne fait pas l'objet d'une contestation. Les mêmes actes des faits prouvés, -couvrent les exigences que cette Chambre a exigé du type de l'art. 172 ter CP, à savoir, l'insistance, la réitération, la répétition, le reflet du même schéma ou modèle systématique, l'existence d'une volonté de persévérer dans ces actions intrusives, dépassant de loin le purement épisodique ou circonstanciel et le manque de légitimation, ou d'autorisation d'agir de cette façon. En raison de la période de temps pendant laquelle ils sont envoyés et de leur contenu, la dévalorisation qu'ils contiennent est d'un niveau très élevé, suffisant pour déclencher une réaction criminelle.

Dans ce cas, il ne s'agit pas d'un simple comportement gênant, les actes décrits dans l'exposé des faits sont susceptibles d'altérer la vie et la tranquillité de la victime de quelque manière que ce soit, d'affecter ou d'altérer l'avenir de la victime de quelque manière que ce soit dans sa vie privée, dans son travail ou dans ses relations avec des tiers. En résumé, Concepción a été soumise à un chantage affectif, entendu comme une forme de communication qui cherche à manipuler une personne sur une autre en utilisant la peur, l'obligation et surtout, dans ce cas, la culpabilité.

Il s'agit de faits qui impliquent une soumission psychologique claire, dans laquelle l'accusé soumet psychologiquement son ex-partenaire avec l'idée qu'il ne cessera pas jusqu'à ce qu'il revienne à lui, le rendant même responsable de sa propre vie avec la tentative d'automutilation dans le jardin de la maison de la victime, qui provoque la peur chez la victime, altérant gravement sa vie quotidienne, qui fait l'objet d'un traitement psychologique, sans qu'il soit nécessaire de fournir au procès une expertise psychologique pour prouver que le psychisme de la victime a été affecté par cette situation de harcèlement ou de stalking, et que cela détermine une altération de sa vie, lorsque, comme en l'espèce, il ressort clairement du récit factuel lui-même, que les événements ont nécessairement généré un impact émotionnel sur la victime - crainte pour sa sécurité et celle de son entourage - et un impact sur le déroulement normal de sa vie quotidienne, avec la nécessité de suivre un traitement psychologique.

Comme nous l'avons dit dans le STS 843/2021 du 4 novembre, l'essence du type de délit, et surtout les actes de violence de genre, tels que le harcèlement dans la situation d'un ancien partenaire, doivent être envisagés dans une perspective de genre, car une situation de harcèlement entre étrangers ou connaissances n'est pas la même que dans la relation d'un partenaire ou d'un ancien partenaire, où les liens interpersonnels créés intensifient les exigences de domination ou d'humiliation du harceleur à l'égard de la victime qui est ou a été son partenaire, afin de créer des liens physiques et psychologiques

qui démontrent la soumission que le harceleur veut transférer à sa victime pour qu'elle ne résiste pas au harcèlement et revienne vers lui.

Par conséquent, les faits décrits sont de nature à contraindre la victime à changer son mode de vie, avec une force suffisante pour constituer un délit de harcèlement tel que défini à l'article 172 ter du code pénal, il y a donc lieu de faire droit à l'appel et de condamner l'accusé, en tant qu'auteur du délit précité, aux mêmes peines que celles prononcées par le tribunal correctionnel, et de rétablir la condamnation précitée.

Conclusions.

Une précision terminologique et factuelle importante de ce type de délit qui, comme l'indique à juste titre le STS 295/2025, ne quantifie pas le nombre d'actes de harcèlement nécessaires pour intégrer l'infraction pénale, mais qui, en tenant compte de l'environnement et en évaluant tous les éléments de preuve dans leur ensemble, et non de manière isolée, permet de l'apprécier parce que le mode de vie de la victime a été altéré, et ce d'autant plus dans les cas de violence à l'égard des femmes.

8 - STS 284/2025, du 27 mars. Abus sexuel sur une jeune fille de 17 ans à l'intelligence limite. Préjudice moral.⁸

Contexte factuel.

Le tribunal correctionnel n° 6 de Las Palmas de Gran Canaria dans l'affaire provenant de l'AP avec le numéro 247/2020, instruit par le tribunal d'instruction n° 1 de Telde, pour un crime d'abus sexuel contre Maximino a émis une sentence qui contient les faits prouvés suivants : "...SOLEIL. Il est prouvé et déclaré que l'accusé, Maximino, né le xx1984, le 1er mai 2017 dans l'après-midi, sans pouvoir préciser l'heure, guidé par le désir de satisfaire ses instincts sexuels, a persuadé la mineure de 17 ans, Socorro, de l'accompagner à l'immeuble situé à l'adresse xxx, et une fois sur place, il lui a touché les fesses et la cuisse, profitant d'elle, sachant qu'elle était mineure et que son niveau de fonctionnement intellectuel était à la limite de l'intelligence normale, ce qui la rendait très vulnérable pour devenir une victime. Le représentant légitime de la mineure prétend...".

En appel, la Cour provinciale a partiellement confirmé l'appel pour retard injustifié et la Cour suprême a confirmé la condamnation de la Cour provinciale.

Base juridique.

D'une part, le requérant fait valoir que les faits sont atypiques en raison du consentement de la victime. La description de l'acte ne permet pas de conclure à un trouble mental. Le jugement parle d'un niveau de fonctionnement intellectuel à la limite de l'intelligence normale. Étant à la limite et non en dessous de la limite - c'est souligné typographiquement - il ne serait pas possible de parler d'abus de trouble.

⁸ STS 284/2025, Penal Sección 1ª, du 27 mars publié sur le site du CGPJ, Centro de Documentación Judicial, CENDOJ. (ROJ : STS 1469/2025 - ECLI:ES:TS:2025:1469), recours : 7022/2022. Orateur : M. Antonio del Moral García.

Le raisonnement n'est pas clair. D'une part, le raisonnement semble indiquer que l'accusé n'était pas au courant de cette circonstance, ce qui est en contradiction avec le fait avéré qu'il a profité de cette caractéristique, ce qui implique la connaissance. Cela contredit le fait avéré qu'il a profité de cette caractéristique, ce qui implique la connaissance. Cela rend l'allégation non viable.

Cela pourrait aussi signifier que, étant à la limite de la normalité, on pourrait parler de normalité, ce qui priverait de soutien l'absence de consentement.

Ce deuxième argument possible joue avec le langage, ignorant le fait que les locutions, intelligence limite ou fonctionnement intellectuel limite, sont des concepts bien ficelés qui expriment quelque chose de plus que ce que l'on pourrait déduire de leur sens littéral strict. Les personnes présentant ces caractéristiques n'ont pas le niveau intellectuel considéré comme moyen. Ce sont - et cela fait partie du patrimoine culturel commun : il ne s'agit pas de psychiatrie, encore moins de technicité juridique - des personnes capables de développer des processus de vie, de fonctionner et de comprendre le monde, mais elles ont besoin d'un soutien approprié, car leur faible QI l'exige. Elles ont des difficultés à prendre des décisions et à résoudre des conflits ; leurs compétences sociales sont réduites. L'Organisation mondiale de la santé établit que l'intelligence moyenne se situe entre 85 et 115 ; les personnes à l'intelligence limite sont celles qui se situent juste en dessous de ces chiffres : entre 70 et 85. On ne peut pas non plus parler de normalité intellectuelle. Du point de vue du droit pénal, ces personnes sont couvertes par le concept normatif de art. 25.1 CP.

Les faits avérés, en outre, comme le montrent encore plus clairement certaines parties du raisonnement factuel, ne mentionnent aucun consentement de la mineure aux attouchements à connotation sexuelle. Il n'est pas dit qu'elle y a consenti. Ils lui ont été imposés jusqu'à ce qu'elle réussisse à s'échapper, mais sans recours à la violence ou à l'intimidation. En fait, le jugement ne cite pas l'article 181.2 (abus de troubles mentaux).

L'accomplissement d'actes sexuels sans le consentement de l'autre personne est typique en soi, quel que soit le niveau intellectuel de la victime. Si, en plus, la victime présente des déficits intellectuels qui la rendent particulièrement vulnérable, l'acte sera aggravé.

La deuxième ligne d'appel cherche à expulser cette aggravation en la considérant comme inhérente à l'abus d'un trouble mental ou indépendante de la volonté de l'accusé.

Ce n'est qu'en déformant les faits avérés que l'on peut soutenir que l'accusé n'était pas conscient de la vulnérabilité particulière découlant de l'intelligence limite qu'il exploitait. Pour le reste, l'enchaînement des faits et la manière dont ils sont restitués dans les motifs juridiques sont extrêmement expressifs.

S'il s'agissait d'un cas où l'on obtient le consentement, exprès ou extériorisé par des actes concluants, de la victime, et que le caractère typique se fonde sur le traitement d'un consentement non libre en raison de l'absence de capacité à le donner et sur le fait que l'auteur profite du déficit cognitif pour l'obtenir, le problème de la compatibilité de l'art. 181.2 ci-dessus (abus de troubles mentaux) ou de l'art. 178.2 en vigueur (abus d'une situation de vulnérabilité de la victime) avec l'aggravation spécifique (particulièrement vulnérable en raison de... l'âge, la maladie, le handicap ou la situation : art. 180.1.3° et

181.5 dans la législation appliquée ; ou vulnérabilité particulière en raison de... le handicap ou toute autre circonstance : art. 180.1.3° après LO 10/2022). Mais ce n'est pas le cas.

D'une part, il y a une absence de consentement. Il ne s'agit pas d'un consentement qui n'est pas libre parce qu'il a été obtenu de manière abusive. D'autre part, il apparaît que la victime a des capacités intellectuelles réduites qui la rendent particulièrement vulnérable.

L'incrimination a donc été correcte.

Et ce qui ressort de la STS, c'est le concept et la portée du dommage moral, si difficile à percevoir dans la pratique quotidienne de nos tribunaux.

A tel point que l'art. 193 CP contient une prescription, dans les condamnations pour crimes contre la liberté sexuelle, outre le prononcé correspondant à la responsabilité civile, il y aura, le cas échéant, ceux correspondant à la filiation et à l'entretien, ce qui représente une présomption légale (basée sur une maxime d'expérience partagée et indubitable) de dommages moraux dans ce type de crime (vid SSTS 327/2013, du 4 mars ; 1033/2013, du 26 octobre ; 733/2016, du 5 octobre ; 812/2017, du 11 décembre ; 393/2020, du 15 juillet ; 1040/2021, du 26 octobre ou 1209/2021, du 2 décembre).

Il ne fait aucun doute pour la requérante qu'une indemnisation serait également accordée devant les tribunaux civils si l'action avait été réservée à ce domaine.

Bien qu'elle ne soit pas applicable car elle n'était pas en vigueur au moment des faits, il est pertinent de se référer à la réglementation de cette question sur Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, car elle soutient, avec des ajouts nouveaux, l'inexcusabilité de cette compensation en décomposant les concepts dans lesquels le préjudice moral et l'atteinte à la dignité sont mis en évidence.

C'est ce que stipule l'article 53 de la loi susmentionnée (), sous le titre "Indemnisation".

"L'indemnisation des dommages matériels et immatériels subis par les victimes de violences sexuelles, conformément aux lois pénales sur la responsabilité civile découlant de l'infraction, doit garantir la satisfaction, économiquement évaluable, au moins des concepts suivants :

(a) les dommages physiques et psychologiques, y compris les dommages moraux et l'atteinte à la dignité.

(b) la perte d'opportunités, notamment en matière d'éducation, d'emploi et d'avantages sociaux.

(c) les dommages matériels et les pertes de revenus, y compris le manque à gagner.

d) Les dommages sociaux, entendus comme des dommages au projet de vie.

e) Traitement thérapeutique, social et de santé sexuelle et reproductive.

2. L'indemnité est versée par la ou les personnes civilement ou pénalement responsables, conformément à la réglementation en vigueur".

Conclusions.

Cette STS 284/2025 traite de deux questions d'intérêt. D'une part, l'adéquation parfaite d'un chiffre aggravé dans les crimes contre la liberté sexuelle, lorsqu'il y a eu un manque de valeur dans l'action de l'agresseur qui n'est pas seulement objective, les actes d'attouchement, mais qui a également une perspective subjective pertinente, profitant sciemment de la vulnérabilité de la victime. D'autre part, le concept presque oublié de préjudice moral, qui, bien qu'existant auparavant dans de nombreuses décisions judiciaires, a été expressément reconnu dans la controversée LO 10/2022 de garantie intégrale de la liberté sexuelle.



Revista Científica
del Centro Universitario
de la Guardia Civil

Revista
Lógos
Guardia Civil

