

# PROJET ARCADIE

EN BREF

ACTUALITÉS

EUROPE

INTERNATIONAL

LES DATAS

RADIO-BUVETTE



Le dernier rapport de la délégation au renseignement révèle l'obsession des services pour vos messages privés, au mépris des risques pour tous les Français.

ACTUALITÉS

## Accès à vos messages privés : la dangereuse obsession du renseignement français

📅 Lundi 04 mai 2026 👤 Tris Acatrinei ⌕ 4 min read

Déposé à la fin de l'année 2025, le rapport d'activité de la **délégation parlementaire au renseignement a été rendu public la semaine dernière.**

Sans réelle surprise, le renseignement français — avec une certaine bienveillance des membres de la délégation — confirme sa volonté d'avoir accès à l'ensemble des messages privés, y compris ceux qui sont chiffrés.

Selon leurs auteurs, pour mener à bien les missions de renseignements et de sécurité, les services doivent pouvoir accéder aux messageries chiffrées. Sans cela, ils ne peuvent pas lutter contre la menace terroriste, le narcotrafic ou les ingérences étrangères. « *L'accès aux contenus chiffrés demeure pourtant un enjeu opérationnel majeur pour les services de renseignement, dans un environnement où 60 % à 80 % des communications transitent désormais par des applications de messagerie chiffrées de bout en bout, tandis que l'usage des SMS et des appels téléphoniques traditionnels reculent* ».

### Un média libre grâce à ses lecteurs

Nous avons fait le choix d'un modèle sans paywall, ni publicité.  
Si l'objectif mensuel est atteint, le média reste entièrement accessible à tous.

Votre soutien permet de rendre cela possible.

[Devenir donateur régulier](#)

## Une ambition ancienne, des obstacles permanents

Diverses tentatives parlementaires avaient eu lieu, mais s'étaient heurtées à la résistance des députés, aussi bien pour des questions de proportionnalité que de faisabilité technique. « *À l'évidence, les conditions de préparation du débat parlementaire sur le sujet du chiffrement, particulièrement à l'Assemblée nationale, n'ont pas permis de dépasser des postures politiques de principe. [...] la Délégation prendra toute sa part au travail de pédagogie nécessaire auprès des parlementaires pour légiférer en connaissance de cause* ».

En somme, les services plaident pour que des dispositions de surveillance des communications soient introduites. L'une des solutions les plus fréquemment évoquées est celle de la porte dérobée ou backdoor. Elle consiste à intégrer dans un système un mécanisme qui permet d'avoir accès aux informations.

Néanmoins, une backdoor ne reste jamais secrète et sera exploitée par des attaquants qui ne seront pas l'État français. Au regard de la sensibilité du sujet, il est évident que si la loi autorise l'introduction d'une backdoor dans des messageries chiffrées, cela rendra ces messageries vulnérables et accessibles à d'autres.

Or, les structures criminelles ciblées par le renseignement s'adapteront, par essence, elles sont agiles et beaucoup plus que les états.

## Une justice européenne jugée encombrante

Au-delà de la question purement technique, la jurisprudence communautaire et européenne impose des contraintes et interdit l'affaiblissement du chiffrement. Pourtant, la délégation qualifie ces jurisprudences de « *déconnectées des réalités techniques et opérationnelles* » et estime qu'elles « *font peser un risque majeur sur la capacité des services de renseignement à conduire leurs investigations* ».

Paradoxalement, les auteurs du rapport occultent une part importante du travail de renseignement, à savoir le renseignement humain et l'infiltration.

Entre les lignes, on comprend que ces techniques sont jugées trop chronophages et trop onéreuses, pour des résultats qui mettent trop de temps à aboutir.

## La France, paradis des leaks

Bien que le rapport ait été rédigé à la fin de l'année 2025, donc avant le **consternant piratage de l'ANTS**, il ne semble pas tenir compte d'une réalité opérationnelle : la France est qualifiée sur les forums spécialisés de paradis de leaks.

En effet, un rapide détour sur Breached ou sur Pwn montre qu'il y a très peu de données personnelles, y compris en provenance de services gouvernementaux, qui ne se retrouvent pas dans la nature. Ainsi, on a pu trouver — sans la consulter — une base de données regroupant des gendarmes, une autre du CROUS, etc.

Mieux encore, par croisement des données, les internautes de ces forums arrivent à établir des profils très détaillés : nom, prénom, date de naissance, profession, adresse postale, email, mots de passe, carte bancaire, opérateur téléphonique, etc. C'est ainsi qu'un plaisantin avait fait croire qu'il avait réussi à **pirater l'Assemblée nationale**, alors qu'il n'avait fait que recycler d'anciennes données.

Cet aspect n'est pas du tout mentionné dans le rapport alors que les faiblesses techniques constituent une cible de choix pour des acteurs étrangers malveillants. À l'inverse, dans les recommandations, la délégation plaide pour « *Engager les adaptations juridiques nécessaires pour faire face à l'élévation du niveau de haute intensité des menaces et de leurs évolutions technologiques* » et demande à être associée « *à la réflexion qu'entend engager le ministère de l'Intérieur sur la lutte contre l'entrisme, au vu de la dimension politique, juridique et technique du sujet* ».

## NIS2, prochain cheval de Troie ?

Cette obsession pour l'affaiblissement généralisée du chiffrement et donc, la compromission des messages privée de tous les utilisateurs explique probablement **pourquoi la transposition de NIS2 n'est toujours pas à l'ordre du jour de l'Assemblée nationale.**

Il apparaîtrait que les services de renseignements souhaiteraient utiliser ce véhicule législatif pour introduire le dispositif des backdoors.

Reste à savoir si leur volonté se traduira lors de l'examen en séance publique.

### 👉 Dans la même rubrique

#### Vidéosurveillance algorithmique : le passage en force au Palais Bourbon

📅 mardi 03 février 2026

#### Données personnelles : LFI demande une commission d'enquête sur les leaks

📅 jeudi 30 avril 2026

#### La vidéosurveillance algorithmique chez les commerçants votée par les députés

📅 lundi 16 février 2026

## Soutenir le Projet Arcadie

Le Projet Arcadie a besoin de financement pour exister. Pour en savoir plus et le soutenir, **cliquez ici** ou via Donorbox si vous souhaitez faire un don défiscalisé ou directement sur la jauge.

Soutenez Arcadie durablement et accédez à notre lettre d'info exclusive.

Objectif : 5100€

Montant actuel : 5021.50€

En bref



LES BRÈVES

## L'ANTS a été piratée par un gamin de 15 ans

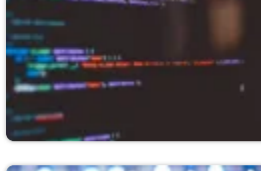
📅 jeudi 30 avril 2026 👤 Tris Acatrinei ⌕ 1 min read

La personne à l'origine du piratage de l'ANTS est un mineur de 15 ans.



### Travail le 1er mai : le projet de loi présenté en conseil des ministres

📅 mercredi 29 avril 2026 ⌕ 2 min read



### Commission d'enquête sur l'audiovisuel : qui a fait fuiter les infos ?

📅 lundi 27 avril 2026 ⌕ 2 min read



### Adoption du rapport sur l'audiovisuel

📅 lundi 27 avril 2026 ⌕ 0 min read



### Antoine Villedieu mis en retrait de son groupe

📅 lundi 27 avril 2026 ⌕ 2 min read

Le dernier rapport

Tout voir



LES RAPPORTS

## Le jeu des ombres : les ingérences étrangères à ciel ouvert

📅 lundi 11 décembre 2023 👤 Tris Acatrinei ⌕ 1 min read

En déclarant une nouvelle fois la guerre à l'Ukraine, Vladimir Poutine ne s'attendait probablement pas à ce que l'Europe s'unisse contre lui. Il nous a pris par surprise alors qu'il n'avait jamais caché ses intentions.

## Les fiches de parlementaires

Vous pouvez retrouver les fiches des parlementaires, les tableaux thématiques et le moteur de recherche croisée, à [cette adresse](#).

Le Projet Arcadie est un média parlementaire, enregistré sous le numéro 0623 Z 94949 auprès de la CPPAP.

Les informations relatives au Projet Arcadie

Les informations financières du Projet Arcadie

Mentions légales

Conditions générales d'utilisation

RGPD - Données personnelles

Recrutements, collaborations et stages

Les sources du Projet Arcadie