23 Voir l'article de la magistrate Laurence Buisson « Risques et périls de l'association de malfaiteurs terroriste » publié en 2017 dans la revue Délibérée (1).

1→ https://www.cairn.info/revue-deliberee-2017-2-page-16.htm?contenu=article

24 Julie Alix et Olivier Cahn, « Mutations de l'antiterrorisme et émergence d'un droit répressif de la sécurité nationale », *Revue de science criminelle et de droit pénal comparé*, 2017.

1→ https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2017-4-page-845.htm

25 Voir note 22

26 Voir note 24

27 Intervention devant le Conseil constitutionnel sur le délit d'« Entreprise individuelle terroriste » en 2017. Une rediffusion (1).

1 → « Entreprise individuelle de terrorisme – Affaire n°2017 625 QPC – Maître François Sureau », 2017, https://www.youtube.com

28 Fédération Internationale des Droits Humains, Rapport « La porte ouverte à l'arbitraire », 1999. Voir aussi le rapport de Human Rights Watch de 2008 intitulé « La justice court-circuitée. Les lois et procédure antiterroristes en France » (1). Voir aussi l'entretien dans Lundi matin avec une personne revenant du Rojava, citée (2), revenant sur la criminalisation de la parole.

1→ « La justice court-circuitée : les lois et procédures anti-terroriste en France », Juillet 2008, https://www.hrw.org/legacy/french/reports/2008/france0708/france0708frwebwcover.pdf
2→ Comité de soutien aux inculpé.es du 8/12, « La logique de l'antiterrorisme : Quelques analyses de base », le 30 Janvier 2022 , sur https://soutien812.net

29 Voir le rapport de la DCPJ du 15 novembre 2008 (1) et les chapitres « Benjamin R. » et « Mathieu B. », pages 109 et 143 du livre *Tarnac, Magasin Général* de David Dufresne (édition de poche).

1→ « Rapport de la sous-direction antiterroriste de la direction centrale de la police judiciaire au procureur de Paris » sur https://web.archive.org/web/20090617014305/https://www.mediapart.fr/files/PV-TGV.pdf

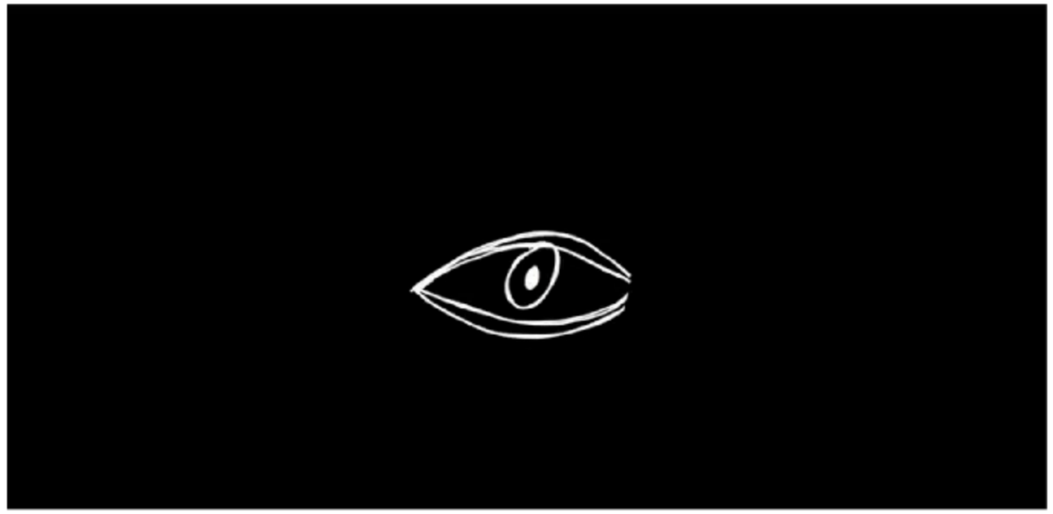
30 Voir notamment l'archive du site des comités de soutien aux inculpé·es de Tarnac (1), une tribune de soutien publiée en 2008 (2) et cette interview (3) de Julien Coupat. Voir aussi le livre de David Dufresne *Tarnac, Magasin Général*.

1→ https://tarnac2018.noblogs.org/
2→ Le Monde, « Non à l'ordre nouveau » , le 27 Novembre 2008, sur https://www.lemonde.fr
3→ Propos recueillis par MANDRAUD Isabelle et MONNOT Caroline , « Julien Coupat : "La prolongation de ma détention est une petite vengeance" », le 25 Mai 2009, sur https://www.lemonde.fr

31 Son audition (1) . Voir à partir de 10:53:50 et 10:55:20 pour les moyens de l'antiterrorisme et à 10:20:19 pour la référence à l'affaire du 8 décembre. Voir aussi sur BFM (2) Gérald Darmanin utiliser l'affaire du 8 décembre pour dénoncer la « *menace d'ultragauche* ».

1→ « Commission des lois, Sainte-Solline, audition de Gérald Darmanin », le 5 Avril 2023, sur https://videos.senat.fr/video.3400114_642d1d98654f8.sainte-soline--audition-de-gerald-darmanin
2→ « Terrorisme: "41 attentats déjoués depuis 2017", dont 9 de l'ultra droite, assure Gérald Darmanin », le 5 Avril 2023, sur https://rmc.bfmtv.com

32 Voir notamment les livres *L'ennemi intérieur. La généalogie coloniale et militaire de l'ordre sécuritaire dans la France contemporaine* de Mathieu Rigouste et *Répression. L'État face aux contestations politiques* de Vanessa Codaccioni.



# Affaire du 8 décembre : Le chiffrement des communications assimilé à un comportement terroriste

*Cet article a été rédigé sur la base d'informations relatives à l'affaire dite du "8 décembre"* [1] *dans laquelle 7 personnes ont été mises en examen pour « association de malfaiteurs terroristes » en décembre 2020. Leur procès est prévu pour octobre 2023. Ce sera le premier procès antiterroriste visant « l'ultragauche » depuis le fiasco de l'affaire Tarnac*[2].

*L'accusation de terrorisme est rejetée avec force par les inculpé·es. Ces dernier·es dénoncent un procès politique, une instruction à charge et une absence de preuves. Ils et elles pointent en particulier des propos décontextualisés et l'utilisation à charge de faits anodins (pratiques sportives, numériques, lectures et musiques écoutées…)*[3]*. De son côté la police reconnaît qu'à la fin de l'instruction – et dix mois de surveillance intensive – aucun « projet précis » n'a été identifié*[4].

*L'État vient d'être condamné pour le maintien à l'isolement du principal inculpé pendant 16 mois et dont il n'a été libéré qu'après une grève de la faim de 37 jours. Une seconde plainte, en attente de jugement, a été déposée contre les fouilles à nu illégales et répétées qu'une inculpée a subies en détention provisoire*[5].

*De nombreuses personnalités, médias et collectifs leur ont apporté leur soutien*[6].

*C'est dans ce contexte que nous avons été alerté du fait que les pratiques numériques des inculpé·es – au premier rang desquelles l'utilisation de messageries chiffrées grand public – sont instrumentalisées comme « preuves » d'une soi-disant « clandestinité » venant révéler l'existence d'un projet terroriste inconnu.*

*Nous avons choisi de le dénoncer.*

16 Voir l'article de Politico (1).

1→CERULUS Laurens, « EU Commission to staff: Switch to Signal messaging app », le 20 Février 2020, sur https://www.politico.eu

17 Voir le rapport du rapporteur des Nations Unies, David Kaye, sur la protection de la liberté d'expression et d'opinion (1). Voir aussi les prises de position de l'Agence national pour la sécurité des systèmes d'information (2), de la Commission nationale de l'informatique et des libertés, et du Conseil National du Numérique (3) ou de l'Agence européenne pour la cybersécurité (4), et le document de l'Observatoire des libertés et du numérique signé notamment par la Ligue des droits de l'Homme, le Syndicat de la magistrature, Amnesty International et le Syndicat des avocats de France (5).

1→United Nation, General Assembly, Human Rights Council, « Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye », le 22 Mai 2015, sur https://lpr.adb.org/sites/default/files/resource/1095/report-on-encryption-anonymity-and-the-human-rights-framework.pdf
2→ PÉPIN Guénaël, « L'ANSSI défend le chiffrement de bout-en-bout, sans portes dérobées », le 3 Août 2016, sur https://www.nextinpact.com
3→ Conseil national du numérique, « Tribune - "Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible" » sur https://cnnumerique.fr
4→ https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto
5→ LQDN, « chiffrement, sécurité et liberté, Positionnement de l'Observatoire de Libertés et du Numérique », Janvier 2017, sur https://www.laquadrature.net

18 Voir le guide de l'hygiène numérique de l'ANSSI préconisant le chiffrement de ses disques durs et disponible (1). Voir aussi la page chiffrement de la CNIL (2) et son guide de chiffrement des données (3).

1→ https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
2→CNIL « Sécurité : Chiffrer, garantir l'intégrité ou signer », sur https://www.cnil.fr
3→CNIL « Comment chiffrer ses documents et ses répertoires ? », sur https://www.cnil.fr

19 Mentionnons les données détenues par les administrations (Assurance maladie, Pôle emploi, les Caisses d'allocations familiales, les URSSAF, les impôts), les fichiers administratifs (permis de conduire, immatriculation, SCA, AGRIPPA), les fichiers de police (notamment le TAJ), les relevés téléphoniques (fadettes). Les réquisitions effectuées par la DGSI auprès des administrations et des entreprises varient selon les inculpé·es. De manière générale, sont contactés Pôle Emploi, la CAF, l'Assurance Maladie, les banques et les opérateurs de téléphonie.

20 En 2020, WhatsApp annonçait compter plus de deux milliards d'utilisateurs et utilisatrices. À ceci s'ajoutent celles et ceux d'autres applications de messageries chiffrées comme Signal, Silence, Wire… Voir cet article (1) du *Monde*.

→ BONAVENTURE Lionel, « WhatsApp franchit la barre des 2 milliards d'utilisateurs », le 12 Février 2020, https://www.lemonde.fr

21 Cette affaire ne fait par ailleurs que confirmer notre opposition, portée devant le Conseil constitutionnel en 2018, à l'obligation de fournir ses codes de déchiffrement et dont nous rappelions récemment l'utilisation massive pour les personnes placées en gardes à vue (1). En plus d'être particulièrement attentatoire à la vie privée et au droit de ne pas s'auto-inscription, cette obligation a, dans cette affaire, été utilisée comme un moyen de pression au maintien des mesures de détention provisoire et même mise en avant pour justifier le refus d'accès au dossier d'instruction à un·e des inculpé·es. A ce sujet voir notre article revenant sur l'utilisation de cette mesure lors des gardes à vue et notre article (2) présentant la question prioritaire de constitutionnalité posée par La Quadrature à ce sujet en 2018.

1→ LQDN, « En GAV, t'es fiché·e ! », 28 avril 2023, https://www.laquadrature.net
2→ LQDN, « Conseil constitutionnel : La Quadrature plaide contre l'obligation de livrer ses clefs de chiffrement », le 6 Mars 2018, sur https://www.laquadrature.net

22 Pauline Le Monnier de Gouville, « De la répression à la prévention. Réflexion sur la politique criminelle antiterroriste », *Les cahiers de la Justice*, 2017 (1).

1→ https://www.cairn.info/revue-les-cahiers-de-la-justice-2017-2-page-209.htm

3→ LQDN, « Mahjoubi et Villani doivent prendre position sur le chiffrement », le 6 Décembre 2017, sur https://www.laquadrature.net
4→ Médiapart, « Le droit à l'anonymat et au chiffrement », sur https://blogs.mediapart.fr « Les enfnats du numérique »
5→ LQDN, « De l'intimité et de sa nécessité », 7 Mars 2016, sur https://www.laquadrature.net
6→ https://gafam.laquadrature.net/
7→ PJL Terrorisme, dernière modification le 25 Mars 2016, sur https://wiki.laquadrature.net
8→ Portail : Loi Renseignement, dernière modification le 11 Janvier 2016, sur https://wiki.laquadrature.net/

11 La criminalisation des pratiques numériques est discutée dans cet article(1) de CQFD par Camille, une inculpée du 8 décembre.

→Camille, inculpée dans l'affaire du 8 décembre 2020, « Ces arrestations sont vouées à semer la peur », sur https://soutien812.net

12 La surveillance généralisée *via* les outils numériques a notamment été révélée par Snowden en 2013 (1). Concernant les enquêtes policières, le discours selon lequel le chiffrement serait un obstacle à leur avancée est pour le moins incomplet. La généralisation du recours au chiffrement ne peut être analysée qu'en prenant en compte le cadre historique de la numérisation de nos sociétés. Cette numérisation s'est accompagnée d'une accumulation phénoménale de données sur chacun·e, et dans une large partie accessibles à la police. Ainsi, le chiffrement ne fait que rétablir un équilibre dans la défense du droit à la vie privée à l'ère numérique. Dans une étude commanditée par le ministère néerlandais de la justice et de la sécurité publiée en 2023 (2), des policiers expliquent clairement ce point : « *Nous avions l'habitude de chercher une aiguille dans une botte de foin et maintenant nous avons une botte de foin d'aiguilles. En d'autres termes, on cherchait des preuves pour une infraction pénale dans le cadre d'une affaire et, aujourd'hui, la police dispose d'un très grand nombre de preuves pour des infractions pénales pour lesquelles des affaires n'ont pas encore été recherchées* ». D'autre part, d'autres techniques peuvent être utilisées pour contourner le chiffrement comme l'expliquait l'Observatoire des libertés et du Numérique en 2017 (3) et la magistrate Laurence Blisson dans l'article « Petits vices et grandes vertus du chiffrement » publié dans la revue Délibérée en 2019.

1→ « Edward Snowden », demière modification le 3 Juin 2023, sur https://fr.wikipedia.org
2→ « Maakt de grote rol van encryptie het opsporingswerk écht anders? », 11 Avril 2023, sur https://www.wodc.nl
3→LQDN, « chiffrement, sécurité et liberté, Positionnement de l'Observatoire de Libertés et du Numérique », Janvier 2017, sur https://www.laquadrature.net
4→ https://www.cairn.info/revue-deliberee-2019-2-page-56.htm

13 La connexion à Tor peut être masquée via l'utilisation de pont (1/2)

1→ https://tb-manual.torproject.org/bridges/
2→ https://orbot.app/en/

14 Pour le chiffrement sur Windows, voir la page Wikipedia de Bitlocker (1) et la documentation de Microsoft (2). Pour le chiffrement sur Android, voir la documentation officielle (3) et l'article de Wire (4). Pour Apple, voir leur documentation ici (5).

1→ « Bitlocker », dernière modification le 13 Mai 2023, sur https://en.wikipedia.org
2→ « Device encryption in Windows », sur https://support.microsoft.com
3→ https://source.android.com/docs/security/features/encryption
4→ NIELD David, « The Android 11 Privacy and Security Features You Should Know », le 27 Septembre 2020, sur https://www.wired.com
5→ « Encryption and Data Protection overview », 18 Février 2021, sur https://support.apple.com

15 Voir le guide pratique du RGPD publié par la CNIL (1). Il y est écrit : « *Le règlement général sur la protection des données (RGPD) précise que la protection des données personnelles nécessite de prendre les "mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque". Cette exigence s'impose aussi bien au responsable du traitement de données personnelles qu'aux sous-traitants impliqués (article 32 du RGPD)* ».

1→ « Guide pratique du RGPD, sécurité des données personnelles », Avril 2023, téléchargeable sur https://www.cnil.fr, par l'intermédiaire de l'article « La CNIL publie une nouvelle version de son guide de la sécurité des données personnelles » du 3 Avril 2023 sur le même site.

*« Tous les membres contactés adoptaient un comportement clandestin, avec une sécurité accrue des moyens de communications (applications cryptées, système d'exploitation Tails, protocole TOR permettant de naviguer de manière anonyme sur internet et wifi public). »*

*DGSI*

*« L'ensemble des membres de ce groupe se montraient particulièrement méfiants, ne communiquaient entre eux que par des applications cryptées, en particulier Signal, et procédaient au cryptage de leurs supports informatiques […]. »*

*Juge d'instruction*

Ces deux phrases sont emblématiques de l'attaque menée contre les combats historiques de La Quadrature du Net dans l'affaire du 8 décembre que sont le droit au chiffrement[7] des communications[8], la lutte contre l'exploitation des données personnelles par les GAFAM[9], le droit à l'intimité et la vie privée ainsi que la diffusion et l'appropriation des connaissances en informatique[10].

Mêlant fantasmes, mauvaise foi et incompétence technique, les éléments qui nous ont été communiqués révèlent qu'un récit policier est construit autour des (bonnes) pratiques numériques des inculpé·es à des fins de mise en scène d'un « *groupuscule clandestin* », « *conspiratif* » et donc… terroriste.

Voici quelques-unes des habitudes numériques qui sont, dans cette affaire, instrumentalisées comme autant de « preuves » de l'existence d'un projet criminel[11]:

**– l'utilisation d'applications comme Signal, WhatsApp, Wire, Silence ou ProtonMail pour chiffrer ses communications ;**

**– le recours à des outils permettant de protéger sa vie privée sur Internet comme un VPN, Tor ou Tails ;**

**– le fait de se protéger contre l'exploitation de nos données personnelles par les GAFAM via des services comme /e/OS, LineageOS, F-Droid ;**

**– le chiffrement de supports numériques ;**

**– l'organisation et la participation à des sessions de formation à l'hygiène numérique ;**

**– la simple détention de documentation technique.**

Alors que le numérique a démultiplié les capacités de surveillance étatiques[12], nous dénonçons le fait que les technologies qui permettent à chacun·e de rétablir un équilibre politique plus que jamais fragilisé soient associées à un comportement criminel à des fins de scénarisation policière.

## Le chiffrement des communications assimilé à un signe de clandestinité

Le lien supposé entre pratiques numériques et terrorisme apparaît dans la note de renseignements à l'origine de toute cette affaire.

Dans ce document, par lequel la DGSI demande l'ouverture d'une enquête préliminaire, on peut lire : « *Tous les membres contactés adoptaient un comportement clandestin, avec une sécurité accrue des moyens de communications (applications cryptées, système d'exploitation Tails, protocole TOR permettant de naviguer de manière anonyme sur internet et wifi public).* »

**Cette phrase apparaîtra des dizaines de fois dans le dossier.** Écrite par la DGSI, elle sera reprise sans aucun recul par les magistrat·es, au premier titre desquels le juge d'instruction mais aussi les magistrat·es de la chambre de l'instruction et les juges des libertés et de la détention.

Durant la phase d'enquête, l'amalgame entre chiffrement et clandestinité est mobilisé pour justifier le déploiement de moyens de surveillance hautement intrusifs comme la sonorisation de lieux privés. La DGSI les juge nécessaires pour surveiller des « *individus méfiants à l'égard du téléphone* » qui « *utilisent des applications cryptées pour communiquer* ».

Après leurs arrestations, les mis·es en examen sont systématiquement questionné·es sur leur utilisation des outils de chiffrement et sommé·es de se justifier : « *Utilisez-vous des messageries cryptées (WhatsApp, Signal, Telegram, ProtonMail) ?* », « *Pour vos données personnelles, utilisez-vous un système de chiffrement ?* », « *Pourquoi utilisez-vous ce genre d'applications de cryptage et d'anonymisation sur internet ?* ». Le lien supposé entre chiffrement et criminalité est clair: ***« Avez-vous fait des choses illicites par le passé qui nécessitaient d'utiliser ces chiffrements et protections ? », « Cherchez-vous à dissimuler vos activités ou avoir une meilleure sécurité ? »***. Au total, on dénombre plus de 150 questions liées aux pratiques numériques.

## Et preuve de l'existence d'*« actions conspiratives »*

À la fin de l'instruction, l'association entre chiffrement et clandestinité est reprise dans les deux principaux documents la clôturant : le réquisitoire du Parquet national antiterroriste (PNAT) et l'ordonnance de renvoi écrite par le juge d'instruction.

Le PNAT consacrera un chapitre entier aux « *moyens sécurisés de communication et de navigation* » au sein d'une partie intitulée… « *Les actions conspiratives* ». Sur plus de quatre pages le PNAT fait le bilan des « preuves » de l'utilisation par les inculpé·es de messageries chiffrées et autres mesures de protection de la vie privée. L'application Signal est particulièrement visée.

Citons simplement cette phrase : ***« Les protagonistes du dossier se caractérisaient tous par leur culte du secret et l'obsession d'une discrétion tant dans leurs échanges, que dans leurs***

1→ « Féministes, nous luttons contre la répression d'État. », téléchargeable sur https://soutien812.net
2→ « L'arrestation de l'un des nôtres, Tribune du collectif des combattantes et combattants francophones du Rojava en soutien à leur camarade incarcéré », téléchargeable sur https://soutienauxinculpeesdu8decembre.noblogs.org
3→ « Antiterrorisme: en grève de la faim, il demande à se défendre dans la dignité », le 9 Avril 2022, sur https://reporterre.net

7 Pour rappel, aujourd'hui le chiffrement est partout. Sur Internet, il est utilisé de manière transparente pour assurer la confidentialité de nos données médicales, coordonnées bancaires et du contenu des pages que nous consultons. Il protège par ailleurs une part croissante de nos communications à travers l'essor des messageries chiffrées comme WhatsApp ou Signal et équipe la quasi-totalité des ordinateurs et téléphones portables vendus aujourd'hui pour nous protéger en cas de perte ou de vol.

8 Le droit au chiffrement des communications, et en particulier le chiffrement de bout en bout (1), c'est-à-dire des systèmes de communications « *où seules les personnes qui communiquent peuvent lire les messages échangés* » dont l'objectif est de « *résister à toute tentative de surveillance ou de falsification* », est régulièrement attaqué par les États au motif qu'il favoriserait la radicalisation politique et constituerait un obstacle majeur à la lutte contre le terrorisme. Récemment, on peut citer un article de Nextinpact (2) décrivant l'appel en avril dernier des services de polices internationaux à Meta (Facebook) pour que Messenger n'intègre pas le chiffrement de bout-en-bout, le projet de loi américain EARN IT (3), les discussions européennes autour du CSAR (4) ou britannique « Online Safety Bill » (5), deux projets qui, par nature, représentent la fin du chiffrement de bout en bout en forçant les fournisseurs de messageries chiffrées à accéder à tout échange pour les vérifier. Une tribune (6) a été publiée le 4 mai dernier, journée de la liberté de la presse, par une quarantaine d'organisations dénonçant ces différents projets. En 2016 et 2017, de nombreuses voix ont réagi aux velléités françaises et allemandes de limiter le chiffrement de bout en bout. À ce sujet, voir notamment cet article de La Quadrature (7), mais aussi les réponses de l'Agence européenne pour la cybersécurité (8) de la CNIL et du Conseil National du Numérique (9) ou encore de l'Agence nationale pour la sécurité des systèmes d'information (10).

1→ « Chiffrement de bout en bout », dernière modification le 30 Mai 2023, sur https://fr.wikipedia.org
2→ MANACH Jean-Marc « Une coalition policière internationale appelle Meta à ne pas étendre le chiffrement de bout en bout », 24 Avril 2023, sur https://www.nextinpact.com
3→ MANACH Jean-Marc, « Le congrès américain s'attaque encore au chiffrement bout en bout », le 8 Février 2022, sur https://www.nextinpact.com
4→ EDRI, « Open Letter : Civil society views on defending privacy while preventing criminal acts », 27 Octobre 2020, sur https://edri.org en tapant dans la barre de recherche du site « Edri open letter csam and encryption » (1er article).
5→ « UK : Online Safety Bill is a serious threat to human rights online », le 25 Avril 2022, sur https://www.article19.org
6→ « Open letter : Protect our rights to privacy, free expression and press freedom », le 3 Mai 2023, sur https://www.fightforthefuture.org
7→ LQDN, « Mahjoubi et Villani doivent prendre position sur le chiffrement », le 6 Décembre 2017, sur https://www.laquadrature.net
8→ « ENISA position on crypto », sur https://www.enisa.europa.eu
9→ « Tribune « chiffrement et lutte contre le terrorisme », attention à ne pas se tromper de cible », le 22 Août 2016, sur https://cnnumerique.fr
10→ PÉPIN Guénaël « L'ANSSI défend le chiffrement de bout en bout, sans portes dérobées », le 3 Août 2016, sur https://www.nextinpact.com

9 Google, Amazon, Facebook, Apple, Microsoft.

10 Parmi les dernières actions de La Quadrature pour le droit au chiffrement et le respect de la vie privée sur Internet, voir notamment notre intervention au Conseil constitutionnel contre l'obligation de donner ses codes de déchiffrement en 2018 (1), contre le règlement de censure terroriste adopté en 2021, nos prises de positions suite aux attaques étatiques contre le chiffrement de bout-en-bout en 2016/2017 (3/4/5), ou encore notre plainte collective (6) contre les GAFAM déposée en 2018. Voir aussi nos prises de positions lors du projet de loi Terrorisme en 2014 (7) et la loi renseignement en 2015 (8).

1→ LQDN, « Conseil constitutionnel : La Quadrature plaide contre l'obligation de livrer ses clefs de chiffrement », 6 Mars 2018, sur https://laquadrature.net
2→ LQDN, « Règlement de censure terroriste adopté : résumons », 7 Mai 2021, sur https://www.laquadrature.net

1 Pour un résumé de l'affaire du 8 décembre voir notamment les témoignages disponibles dans cet article de la Revue Z(1). Cet article de Lundi matin (2). Les articles des comités de soutien suivants (3/4/5) et la page Wikipedia (6)

1→Camille, « La taule a réduit mon corps à son plus petit souffle », article paru dans la revue Z, et téléchargeable sur le blog https://soutien812.net
2→ "Affaire du 8 décembre : récit d'une mise en examen pour association de malfaiteurs terroriste », le 28 Février 2022 sur https://lundi.am
3→ « Un récit de l'affaire du 8/12 », le 30 Janvier 2022, sur https://soutien812.net
4→ « 10 mois derrière les barreaux pour des inculpé.es du 8 décembre », le 28 Octobre 2021 , sur https://soutienauxinculpeesdu8decembre.noblogs.org
5→ « Après les peines, l'heure du châtiment ? », le 20 Septembre 2022, sur https://soutien812.net
6→ « Affaire du 8 décembre 2020 », dernière mise à jour le 7 Juin 2023, sur https://fr.wikipedia.org

2 L'affaire de Tarnac est un fiasco judiciaire de l'antiterrorisme français. Les inculpé·es ont tous et toutes été relaxé·es après dix années d'instruction. C'est la dernière affaire antiterroriste visant les mouvements de gauche en France. Résumé de l'affaire de Tarnac (1)

1→ « Affaire de Tarnac », dernière mise à jour le 2 Juin 2023 , sur https://fr.wikipedia.org

3 Voir cette lettre ouverte au juge d'instruction (1), cette lettre de Libre Flot au moment de commencer sa grève de la faim (2), cette compilation de textes publiés en soutien aux inculpé·es (3), l'émission de Radio Pikez (4) et celle de Radio Parleur (5). Un article du Monde Diplomatique d'avril 2021 (6) et les articles publiés sur les sites des comités de soutien (7/8)

1→ « Lettre ouverte au juge d'instruction Jean-Marc Herbaut », le 8 Septembre 2021, sur https://soutienauxinculpeesdu8decembre.noblogs.org
2→ Libre Flot, « Pourquoi je fais la grève de la faim », le 27 Février 2022, sur https://soutien812.net
3→ « Les inculpé.es du 8 Décembre 2020 », téléchargeable sur https://soutienauxinculpeesdu8decembre.noblogs.org
4→ Radio Pikez, « Antiterrorisme et Désinformation », le 10 Novembre 2021, sur https://soutienauxinculpeesdu8decembre.noblogs.org
5→ « Libre Flot, 37 jours de grève de la faim », le 13 Avril 2022, sur https://radioparleur.net
6→ Le Monde diplomatique « Combattre les djihadistes, un crime? », le 2 Avril 2021, sur https://soutienauxinculpeesdu8decembre.noblogs.org
7→ https://soutien812.blackblogs.org/
8→ https://soutienauxinculpeesdu8decembre.noblogs.org/

4 Voir notamment cet article du monde (1)

1→ SAMUEL Laurent « Sept militants de l'ultragauche mis en examen pour « association de malfaiteurs terroriste », le 11 décembre 2020, sur https://www.lemonde.fr

5 Sur les recours déposés par Camille et LibreFlot, voir le communiqué de presse (1). Sur la condamnation de l'État sur le maintien illégal à l'isolement de LibreFlot, voir l'article de Reporterre (2) et de Ouest-France (3). Sur ses conditions de vie à l'isolement et sa grève de la faim, voir notamment cette compilation (4) d'écrits de Libre Flot et le témoignage joint au communiqué de presse évoqué ci-avant.

1→« L'État attaqué en justice pour atteinte à la dignité humaine », le 2 Avril 2023, sur https://soutien812.net
2→ « L'État condamné pour avoir maintenu un militant emprisonné à l'isolement », le 5 Mai 2023, sur https://reporterre.net
3→ « Prison: le maintien à l'isolement d'un détenu d'ultragauche était illégal », sur https://www.ouestfrance.fr
4→ « Libre Flot, du quartier d'isolement à la grève de la faim, Centre Pénitentiaire de Bois d'Arcy (2021-2022), sur https://soutien812.net

6 Voir la tribune de soutien signée plusieurs collectifs et intellectuelles féministes (1), la tribune de soutien du collectif des combattantes et combattants francophones du Rojava (2) et la tribune de soutien signée par plusieurs médias et personnalités (3)

***navigations sur internet. L'application cryptée signal était utilisée par l'ensemble des mis en examen, dont certains communiquaient exclusivement [surligné dans le texte] par ce biais.* ».**

Le juge d'instruction suivra sans sourciller en se livrant à un inventaire exhaustif des outils de chiffrement qu'ont « *reconnu* » – il utilisera abondamment le champ lexical de l'aveu – utiliser chaque mis·e en examen : « *Il reconnaissait devant les enquêteurs utiliser l'application Signal* », « *X ne contestait pas utiliser l'application cryptée Signal* », « *Il reconnaissait aussi utiliser les applications Tails et Tor* », « *Il utilisait le réseau Tor […] permettant d'accéder à des sites illicites* ».

## Criminalisation des connaissances en informatique

Au-delà du chiffrement des communications, ce sont aussi les connaissances en informatique qui sont incriminées dans cette affaire : elles sont systématiquement assimilées à un facteur de « dangerosité ».

La note de la DGSI, évoquée ci-dessus, précise ainsi que parmi les « *profils* » des membres du groupe disposant des « *compétences nécessaires à la conduite d'actions violentes* » se trouve une personne qui posséderait de « *solides compétences en informatique et en communications cryptées* ». Cette personne et ses proches seront, après son arrestation, longuement interrogé·es à ce sujet.

Alors que ses connaissances s'avéreront finalement éloignées de ce qu'avançait la DGSI – elle n'est ni informaticienne ni versé·e dans l'art de la cryptographie – **le juge d'instruction n'hésitera pas à inscrire que cette personne a « *installé le système d'exploitation Linux sur ses ordinateurs avec un système de chiffrement* »**. Soit un simple clique sur « oui » quand cette question lui a été posée lors de l'installation.

La simple détention de documentation informatique est elle aussi retenue comme un élément à charge. Parmi les documents saisis suite aux arrestations, et longuement commentés, se trouvent des notes manuscrites relatives à l'installation d'un système d'exploitation grand public pour mobile dégooglisé (/e/OS) et mentionnant diverses applications de protection de la vie privée (GrapheneOS, LineageOS, Signal, Silence, Jitsi, OnionShare, F-Droid, Tor, RiseupVPN, Orbot, uBlock Origin…).

Dans le procès-verbal où ces documents sont analysés, un·e agent·e de la DGSI écrit que « *ces éléments confirment* [une] *volonté de vivre dans la clandestinité.* ». Le PNAT suivra avec la formule suivante : « *Ces écrits constituaient un véritable guide permettant d'utiliser son téléphone de manière anonyme, confirmant la volonté de X de s'inscrire dans la clandestinité, de dissimuler ses activités […].* ».

Ailleurs, la DGSI écrira que **« […] *la présence de documents liés au cryptage des données informatiques ou mobiles [dans un scellé]* »** matérialisent **« *une volonté de communiquer par des moyens clandestins.* »**.

## Et de leur transmission

L'incrimination des compétences informatiques se double d'une attaque sur la transmission de ces dernières. Une partie entière du réquisitoire du PNAT, intitulée « *La formation aux moyens de communication et de navigation sécurisée* », s'attache à criminaliser les formations à l'hygiène numérique, aussi appelées « Chiffrofêtes » ou « Cryptoparties ».

Ces pratiques collectives et répandues – que La Quadrature a souvent organisées ou relayées – contribuent à la diffusion des connaissances sur les enjeux de vie privée, de sécurisation des données personnelles, des logiciels libres et servent à la réappropriation de savoirs informatiques par toutes et tous.

Qu'est-il donc reproché à ce sujet dans cette affaire ? Un atelier de présentation de l'outil Tails*, système d'exploitation grand public prisé des journalistes et des défenseurs·ses des libertés publiques. **Pour le PNAT c'est lors de cette formation que « *X les a dotés de logiciels sécurisés et les a initiés à l'utilisation de moyens de communication et de navigation internet cryptés, afin de leur garantir l'anonymat et l'impunité* ». Le lien fait entre droit à la vie privée et impunité, corollaire du fantasme policier d'une transparence totale des citoyen·nes, a le mérite d'être clair.**

Le PNAT ajoutera: « *X ne se contentait pas d'utiliser ces applications* [de protection de la vie privée], *il apprenait à ses proches à le faire* ». Phrase qui sera reprise, mot pour mot, par le juge d'instruction.

**Pire, ce dernier ira jusqu'à retenir cette formation comme un des « *faits matériels* » caractérisant « *la participation à un groupement formé* […] *en vue de la préparation d'actes de terrorisme* »,** tant pour la personne l'ayant organisé – « *en les formant aux moyens de communication et de navigation internet sécurisés* » – que pour celles et ceux l'ayant suivi – « *en suivant des formations de communication et de navigation internet sécurisés* ».

De son côté, la DGSI demandera systématiquement aux proches des mis·es en examen si ces dernier·es leur avaient recommandé l'utilisation d'outils de chiffrement : « *Vous ont-ils suggéré de communiquer ensemble par messageries cryptées ?* », « *C'est lui qui vous a demandé de procéder à l'installation de SIGNAL* ? ».

**Une réponse inspirera particulièrement le PNAT qui écrira : « *Il avait convaincu sa mère d'utiliser des modes de communication non interceptables comme l'application Signal.* »**

## « Êtes-vous anti-GAFA? »

**Même la relation à la technologie et en particulier aux GAFAM – contre lesquels nous sommes mobilisés depuis de nombreuses années – est considérée comme un signe de radicalisation**. Parmi les questions posées aux mis·es en examen, on peut lire : « *Etes-vous anti GAFA ?* », « *Que* utilisent « *Signal, WhatsApp, Telegram* » en des termes sans équivoque: « *Donnez-nous pour la violence des extrêmes les mêmes moyens que le terrorisme* ».

Pour se justifier, il avançait qu'il existe « *une paranoia avancée très forte dans les milieux d'ultragauche* […] *qui utilisent des messageries cryptées* » ce qui s'expliquerait par une « *culture du clandestin* ». Un véritable copier-coller de l'argumentaire policier développé dans l'affaire du 8 décembre. Affaire qu'il citera par ailleurs – au mépris de toute présomption d'innocence – comme l'exemple d'un « *attentat déjoué* » de « *l'ultragauche* »[31] pour appuyer son discours visant à criminaliser les militant·es écologistes.

Voici comment la criminalisation des pratiques numériques s'inscrit dans la stratégie gouvernementale de répression de toute contestation sociale. **Défendre le droit au chiffrement, c'est donc s'opposer aux dérives autoritaires d'un pouvoir cherchant à étendre, sans fin, les prérogatives de la lutte « antiterroriste » *via* la désignation d'un nombre toujours plus grand d'ennemis intérieurs**[32].

Après la répression des personnes musulmanes, des « *écoterroristes* », des « *terroristes intellectuels* », voici venu la figure des terroristes armé·es de messageries chiffrées. Devant une telle situation, la seule question qui reste semble être : **« Et toi, quel·le terroriste es-tu ? »***.

---

* https://tails.boum.org/

* "SUPER BINGO ! Quel terroriste d'ultragauche es-tu ? » , le 4 Janvier 2023, sur https://paris-luttes.info

## Antiterrorisme, chiffrement et justice préventive

Il n'est pas possible de comprendre l'importance donnée à l'association de pratiques numériques à une soi-disant clandestinité sans prendre en compte le basculement de la lutte antiterroriste « *d'une logique répressive à des fins préventives* »[22] dont le délit « *d'association de malfaiteurs terroristes en vue de* » (AMT) est emblématique[23]. Les professeur·es Julie Alix et Oliver Cahn[24] évoquent une « *métamorphose du système répressif* » d'un droit dont l'objectif est devenu de « *faire face, non plus à une criminalité, mais à une menace* ».

Ce glissement vers une justice préventive « *renforce l'importance des éléments recueillis par les services de renseignements* »[25] qui se retrouvent peu à peu libres de définir qui représente une menace « *selon leurs propres critères de la dangerosité* »[26].

**Remplacer la preuve par le soupçon, c'est donc substituer le récit policier aux faits.** Et ouvrir la voie à la criminalisation d'un nombre toujours plus grands de comportements « *ineptes, innocents en eux-mêmes* »[27] pour reprendre les mots de François Sureau. Ce que critiquait déjà, en 1999, la Fédération internationale des droits humains qui écrivait que « *n'importe quel type de "preuve", même insignifiante, se voit accorder une certaine importance* »[28].

Et c'est exactement ce qu'il se passe ici. Des habitudes numériques répandues et anodines sont utilisées à charge dans le seul but de créer une atmosphère complotiste supposée trahir des intentions criminelles, aussi mystérieuses soient-elles. Atmosphère dont tout laisse à penser qu'elle est, justement, d'autant plus nécessaire au récit policier que les contours des intentions sont inconnus.

À ce titre, il est particulièrement frappant de constater que, si la clandestinité est ici caractérisée par le fait que les inculpé·es feraient une utilisation « avancée » des outils technologiques, elle était, dans l'affaire Tarnac, caractérisée par le fait… de ne posséder aucun téléphone portable[29]. Pile je gagne, face tu perds[30].

## Toutes et tous terroristes

À l'heure de conclure cet article, l'humeur est bien noire. Comment ne pas être indigné·e par la manière dont sont instrumentalisées les pratiques numériques des inculpé·es dans cette affaire ?

Face au fantasme d'un État exigeant de toute personne une transparence totale au risque de se voir désignée comme « suspecte », nous réaffirmons le droit à la vie privée, à l'intimité et à la protection de nos données personnelles. Le chiffrement est, et restera, un élément essentiel pour nos libertés publiques à l'ère numérique.

Soyons clair: cette affaire est un test pour le ministère de l'intérieur. Quoi de plus pratique que de pouvoir justifier la surveillance et la répression de militant·es parce qu'ils et elles utilisent WhatsApp ou Signal?

Auditionné par le Sénat suite à la répression de Sainte-Soline, Gérald Darmanin implorait ainsi le législateur de changer la loi afin qu'il soit possible de hacker les portables des manifestant·es qui *pensez-vous des GAFA ?* » ou encore « *Eprouvez-vous une certaine réserve vis-à-vis des technologies de communication ?* ».

Ces questions sont à rapprocher d'une note de la DGSI intitulée « *La mouvance ultra gauche* » selon laquelle ses « *membres* » feraient preuve « *d'une grand culture du secret* […] *et une certaine réserve vis-à-vis de la technologie* ».

C'est à ce titre que le système d'exploitation pour mobile dégooglisé et grand public /e/OS* retient particulièrement l'attention de la DGSI. Un SMS intercepté le mentionnant sera longuement commenté. Le PNAT indiquera à son sujet qu'un·e inculpé·e s'est renseigné·e à propos d'un « *nouveau système d'exploitation nommé /e/* […] *garantissant à ses utilisateurs une intimité et une confidentialité totale* ».

En plus d'être malhonnête – ne pas avoir de services Google n'implique en rien une soi-disante « *confidentialité totale* » – ce type d'information surprend dans une enquête antiterroriste.

## Une instrumentalisation signe d'incompétence technique ?

Comment est-il possible qu'un tel discours ait pu trouver sa place dans un dossier antiterroriste ? Et ce sans qu'aucun des magistrat·es impliqué·es, en premier lieu le juge d'instruction et les juges des libertés et de la détention, ne rappelle que ces pratiques sont parfaitement légales et nécessaires à l'exercice de nos droits fondamentaux ? Les différentes approximations et erreurs dans les analyses techniques laissent penser que le manque de compétences en informatique a sûrement facilité l'adhésion générale à ce récit.

À commencer par celles de la DGSI elle-même, dont les rapports des deux centres d'analyses techniques se contredisent sur… le modèle du téléphone personnel du principal inculpé.

Quant aux notions relatives au fonctionnement de Tor** et Tails, bien qu'au centre des accusations de « *clandestinité* », elles semblent bien vagues.

Un·e agent·e de la DGSI écrira par exemple, semblant confondre les deux : **« *Thor* [sic] *permet de se connecter à Internet et d'utiliser des outils réputés de chiffrement de communications et des données. Toutes les données sont stockées dans la mémoire RAM de l'ordinateur et sont donc supprimées à l'extinction de la machine* ».** Ne serait-ce pas plutôt à Tails que cette personne fait allusion?

Quant au juge d'instruction, il citera des procès verbaux de scellés relatifs à des clés Tails, qui ne fonctionnent pas sur mobile, comme autant de preuves de connaissances relatives à des « *techniques complexes pour reconfigurer son téléphone afin de le rendre anonyme* ». Il ajoutera par ailleurs, tout comme le PNAT, que Tor permet de « *naviguer anonymement sur internet grâce au wifi public* » – comme s'il pensait qu'un wifi public était nécessaire à son utilisation.

La DGSI, quant à elle, demandera en garde à vue les « *identifiants et mots de passe pour Tor* » – qui n'existent pas – et écrira que l'application « *Orbot* », ou « *Orboot* » pour le PNAT, serait « *un serveur 'proxy' TOR qui permet d'anonymiser la connexion à ce réseau* ». Ce qui n'a pas de sens. Si

* https://e.foundation/e-os/
** https://www.torproject.org/

Orbot permet bien de rediriger le trafic d'un téléphone *via* Tor, il ne masque en rien l'utilisation faite de Tor[13].

Les renseignements intérieurs confondent aussi Tails avec le logiciel installé sur ce système pour chiffrer les disques durs – appelé LUKS – lorsqu'elle demande: « *Utilisez vous le système de cryptage "Tails" ou "Luks" pour vos supports numériques ?* ». S'il est vrai que Tails utilise LUKS pour chiffrer les disques durs, Tails est un système d'exploitation – tout comme Ubuntu ou Windows – et non un « *système de cryptage* ». Mentionnons au passage les nombreuses questions portant sur « *les logiciels cryptés (Tor, Tails)* ». Si Tor et Tails ont bien recours à des méthodes chiffrement, parler de « *logiciel crypté* » dans ce contexte n'a pas de sens.

Notons aussi l'utilisation systématique du terme « *cryptage* », au lieu de « chiffrement ». Si cet abus de langage – tel que qualifié par la DGSI sur son site* – est commun, il trahit l'amateurisme ayant conduit à criminaliser les principes fondamentaux de la protection des données personnelles dans cette affaire.

Que dire enfin des remarques récurrentes du juge d'instruction et du PNAT quant au fait que les inculpé·es chiffrent leurs supports numériques et utilisent la messagerie Signal ?

**Savent-ils que la quasi-totalité des ordinateurs et téléphones vendus aujourd'hui sont chiffrés par défaut[14]**? Les leurs aussi donc – sans quoi cela constituerait d'ailleurs une violation du règlement européen sur la protection des données personnelles[15].

**Quant à Signal, accuseraient-ils de clandestinité la Commission Européenne qui a, en 2020, recommandé son utilisation à son personnel[16]?** Et rangeraient-ils du côté des terroristes le rapporteur des nations Unies qui rappelait en 2015 l'importance du chiffrement pour les droits fondamentaux[17] ? Voire l'ANSSI et la CNIL qui, en plus de recommander le chiffrement des supports numériques osent même… mettre en ligne de la documentation technique pour le faire[18] ?

En somme, nous ne pouvons que les inviter à se rendre, plutôt que de les criminaliser, aux fameuses « Chiffrofêtes » où les bases des bonnes pratiques numériques leur seront expliquées.

## Ou nécessité d'un récit policier ?

Si un tel niveau d'incompétence technique peut permettre de comprendre comment a pu se développer un fantasme autour des pratiques numériques des personnes inculpé·es, cela ne peut expliquer pourquoi elles forment le socle du récit de « *clandestinité* » de la DGSI.

Or, dès le début de l'enquête, la DGSI détient une quantité d'informations considérables sur les futur·es mis·es en examen. À l'ère numérique, elle réquisitionne les données détenues par les administrations (Caf, Pôle Emploi, Ursaff, Assurance-Maladie…), consulte les fichiers administratifs (permis de conduire, immatriculation, SCA, AGRIPPA), les fichiers de police (notamment le TAJ) et analyse les relevés téléphoniques (fadettes). Des réquisitions sont envoyées à de nombreuses entreprises (Blablacar, Air France, Paypal, Western Union…) et le détail des comptes bancaires est minutieusement analysé[19].

* https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/glossaire/glossaire

À ceci s'ajoutent les informations recueillies *via* les mesures de surveillances ayant été autorisées – comptant parmi les plus intrusives que le droit permette tel la sonorisation de lieux privés, les écoutes téléphoniques, la géolocalisation en temps réel *via* des balises gps ou le suivi des téléphones, les IMSI catcher – et bien sûr les nombreuses filatures dont font l'objet les « *cibles* ».

Mais, alors que la moindre interception téléphonique évoquant l'utilisation de Signal, WhatsApp, Silence ou Protonmail fait l'objet d'un procès-verbal – assorti d'un commentaire venant signifier la « *volonté de dissimulation* » ou les « *précautions* » témoignant d'un « *comportement méfiant* » – comment expliquer que la DGSI ne trouve rien de plus sérieux permettant de valider sa thèse parmi la mine d'informations qu'elle détient ?

La DGSI se heurterait-elle aux limites de son amalgame entre pratiques numériques et clandestinité ? Car, de fait, **les inculpé·es ont une vie sociale, sont déclarées auprès des administrations sociales, ont des comptes bancaires, une famille, des ami·es, prennent l'avion en leur nom, certain·es travaillent, ont des relations amoureuses…**

En somme, les inculpé·es ont une vie « normale » et utilisent Signal. Tout comme les plus de deux milliards d'utilisateurs et utilisatrices de messageries chiffrées dans le monde[20]. Et les membres de la Commission européenne…

## Chiffrement et alibi policier

La mise en avant du chiffrement offre un dernier avantage de choix au récit policier. Elle sert d'alibi pour expliquer l'absence de preuves quant à l'existence d'un soi-disant projet terroriste. Le récit policier devient alors : **ces preuves existent, mais elles ne peuvent pas être déchiffrées**.

Ainsi le juge d'instruction écrira que si les écoutes téléphoniques n'ont fourni que « *quelques renseignements utiles* », ceci s'explique par « *l'usage minimaliste de ces lignes* » au profit d'« *applications cryptées, en particulier Signal* ». **Ce faisant, il ignore au passage que les analyses des lignes téléphoniques des personnes inculpées indiquent une utilisation intensive de SMS et d'appels classiques pour la quasi-totalité d'entre elles.**

Ce discours est aussi appliqué à l'analyse des scellés numériques dont l'exploitation n'amène pas les preuves tant espérées. Suite aux perquisitions, la DGSI a pourtant accès à tout ou partie de six des sept téléphones personnels des inculp·ées, à cinq comptes Signal, à la majorité des supports numériques saisis ainsi qu'aux comptes mails et réseaux sociaux de quatre des mis·es en examen. **Soit en tout et pour tout des centaines de gigaoctets de données personnelles, de conversations, de documents. Des vies entières mises à nu, des intimités violées pour être offertes aux agent·es des services de renseignements**.

Mais rien n'y fait. Les magistrat·es s'attacheront à expliquer que le fait que trois inculpé·es refusent de fournir leurs codes de déchiffrement – dont deux ont malgré tout vu leurs téléphones personnels exploités grâce à des techniques avancées – entrave « *le déroulement des investigations* » et empêche « *de caractériser certains faits* ». **Le PNAT ira jusqu'à regretter que le refus de communiquer les codes de déchiffrement empêche l'exploitation… d'un téléphone cassé et d'un téléphone non chiffré**. Après avoir tant dénoncé le complotisme et la « *paranoïa* » des inculpé·es, ce type de raisonnement laisse perplexe[21].