

Objet : Lettre ouverte à l'attention de la population et aux représentants élus de la république française concernant les divers projets de lois en lien avec le numérique.

Madame, Monsieur,

Cela fait maintenant plusieurs mois voire années que des élus de la république française, et certaines représentants en Europe, tentent de proposer des projets de lois visant à élargir le « contrôle numérique » et restreindre les libertés fondamentales inhérentes. Ainsi, nous listons les mesures les plus récentes dans ce qui suit :

1. Tentative d'amendement n°CS553 [1] au Projet de loi n°1514

Visant à sécuriser et réguler l'espace numérique et suivi par bon nombre de députés, qui traite du sujet des « VPN » ou RPV (Réseau Privé Virtuel), et bien au delà de ce qu'il prétend être réduit aux simples réseaux sociaux.

Amendement retiré, ce qui n'empêche pas de revoir un jour ce type de texte et de montrer la totale déconnexion de nombreux élus avec leur population et l'économie de leur pays :

Les RPV, au sens large, sont utilisés couramment par bon nombres d'entreprises afin de sécuriser leurs échanges (intranet mais aussi et surtout inter-sites) y compris lors des investigations (réputation en ligne et détection de menaces éventuelles) réalisées sur lesdits réseaux sociaux. Comme le fait à notre connaissance un partenaire privilégié de l'État, par le biais de ses Centres de Services Mutualisés des Services d'Information (CSMSI), ce qui dans ce cas reviendrait à un « tir ami » !

L'ANSSI fait par ailleurs ses recommandations en faveur de cet outil de sécurisation, dans son guide « Recommandations sur le nomadisme numérique » [2]. L'administration elle-même dispose de son propre guide, disponible auprès de l'ANSSI [3], qui mentionne l'usage de RPV dans les contextes de nomadisme et d'administration à distance, directives qui de notre expérience ne sont que trop peu suivies par les administrations. De plus, comme le souligne un de nos confrères dans l'article de France 3 Régions [4] : les RPV « [sont utilisés] par les forces de l'ordre dans leurs enquêtes, et par tous les professionnels de la cybersécurité. Dans certains pays, ils sont même recommandés pour passer outre la censure ou par mesure de sécurité ».

Les élus chercheraient-ils à fragiliser l'économie numérique, ainsi que l'administration française ?

Voici, à ce jour, pour information, la liste des pays qui appliquent un blocage ou une restriction sur ce type d'outil [5] :

- Restreint (à des degrés divers) : Chine, Émirats Arabes Unis, Oman, Ouganda, Russie, Venezuela
- Considéré illégal : Biélorussie, Corée du Nord, Irak

La France se doit d'être exemplaire face à ces régimes : interdire ou limiter l'utilisation des RPV serait non seulement une énième « usine à gaz », mais également une renonciation aux principes républicains qui nous différencient de ces régimes autoritaires.

2. Article 6 du Projet de loi n°1514 [6]

Visant à sécuriser et réguler l'espace numérique, qui tente d'imposer aux développeurs d'applications de navigateur internet, un outil pour bloquer des contenus de sites figurant sur une liste fournie par le gouvernement, et annoncés comme étant liés à de la fraude en ligne.

Nous attendons de nos élus et leurs conseillers qu'ils se consacrent à aider nos concitoyens à mieux naviguer sur les réseaux plutôt que de s'aventurer sur un sujet qu'ils ne maîtrisent pas, en appliquant une censure que bon nombres de régimes autoritaires utilisent.

Même si le sujet a été récemment amendé, du fait entre autre qu'une fondation ait publié un billet (du 27 juin 2023 [7]) ainsi qu'une pétition (en ligne [8]), il est entendu qu'une telle possibilité technique offerte à un gouvernement, permettrait d'ajuster par la suite la norme à sa guise et ôterait tout garde-fou en matière de protection de la liberté d'expression.

3. Amendement n°CS597 [9] du projet de loi 1514

Visant à sécuriser et réguler l'espace numérique.

Questionner tous les français par voie de référendum sur leur souhait ou non d'adopter cette mesure serait une démarche politique louable.

Lier une identité numérique à nos actes en ligne sur les réseaux sociaux est un principe, non seulement contraire à l'expression libre, mais également source potentielle de collusion avec des entités privées éloignées de l'intérêt collectif¹. Nous questionnons également l'élargissement de cette identité numérique à l'espace réel, via la « e-carte d'identité » : stockée dans des applications tierces dites de « portefeuille numérique² », tenues par des entités privées ; entités qui au passage n'ont pas investi tant d'énergie dans le développement de ces outils dans un but purement altruiste et démocratique. L'identité numérique permettrait de collecter une trace constante de l'intégralité de nos interactions, en tout lieu, et cela pourrait être l'occasion d'atteintes multiples : au secret médical, à la liberté de circuler, à la liberté d'opinion, à la liberté de s'autodéterminer, entre autres...

Par ailleurs, nous dénonçons la caricature faite par cet amendement concernant l'anonymat (en ligne), qui consiste à définir son utilisation à des fins malveillantes ou participant d'une volonté criminelle. Nous entendons par anonymat la « possibilité de ne pas être constamment surveillé, pisté et contrôlé en tous lieux » par anticipation ou présomption d'un comportement supposé préjudiciable (les enquêtes criminelles, légitimes, faisant exception) ; ou même la possibilité de s'exprimer librement, sans crainte de censure, de contraintes géographiques et physiques, ou de représailles d'une quelconque nature (y compris politique). Ce droit à l'anonymat est par ailleurs défendu par le rapporteur spécial M. David Kaye dans le livrable [10] remis aux représentants des Nations Unies.

Finalement, l'encadrement annoncé pour cette solution pourrait - si l'envie en prenait aux divers successeurs de la scène gouvernementale à l'avenir - être contourné via les voies officieuses ; cela s'est déjà passé à de multiples reprises. Le débat est biaisé par l'absence d'informations loyales sur ces sujets. Toute personne versée dans la question numérique et son éthique vous le soutiendra : le tout informatisé sécuritaire, garant des libertés publiques est une chimère, en plus d'un « mensonge par omission ». Tant à travers son accaparement par les intérêts privés, que par le fait qu'en ligne rien n'est et ne pourra être totalement sécurisé et rien n'est et ne pourra être intégralement sous contrôle. La justice ne doit pas être substituée par le « pré-crime », source de déstabilisation des principes démocratiques.

4. Les attaques successives sur les outils à sources ouvertes (dits « open source »)

Non seulement du gouvernement français actuel, plus largement d'une partie de la classe politique mais aussi d'autres gouvernements européens, dont le point d'orgue est le projet européen « Cyber Resilience Act » [11].

Ces attaques sont intolérables envers les bénévoles qui donnent de leur temps afin de produire ces outils et nous attendons de nos élus qu'ils aient enfin le courage de dénoncer ces agissements et ces projets grotesques.

Nous nous faisons une fois encore l'écho de bon nombre d'articles publiés par des personnes plus compétentes que les bureaucrates qui ont proposé ce projet. Par exemple l'APRIL [12], la CNLL [13]. Et bien d'autres fondations et associations représentant les travailleurs de ce domaine qui vous ont adressé une lettre ouverte [14], semble-t-il restées lettre morte !

Nous rappelons que ces logiciels à sources ouvertes sont la base d'une partie non négligeable des logiciels que vous utilisez au quotidien, y compris vos logiciels privateurs. Et que ce secteur d'activité emploie une myriade de techniciens, d'ingénieurs et doctorants qui souvent prennent sur leur temps libre pour améliorer sans cesse ces outils et les sécuriser. Employés qui dans leur cas créent une grande valeur ajoutée à nos sociétés, en plus du côté éthique.

5. La loi n° 2021-998 du 30 juillet 2021 [15]

Relative à la prévention d'actes de terrorisme et au renseignement, dénoncée de toutes parts comme par exemple dans un billet [16] et notamment par un courrier d'associations, avocats, syndicats et universitaires [17]. Pourtant bien votée, en procédure accélérée, sans que nos élus n'aient intercédé et sans que le peuple n'ait pu débattre réellement du sujet.

Cette façon de faire est une attaque directe contre le peuple, non seulement français mais européen.

1 Sociétés gravitant supposément autour de la « Tech », que ce soit civile et/ou militaire, dont le modèle économique repose déjà sur la collecte et la monétisation des données personnelles, ou qui ambitionnent cette « part du gâteau ».

2 Application centralisation de façon indifférenciée : données d'identité, données bancaires, d'assurance, de santé et administratives. Tous ses œufs dans le même panier, peut-on qualifier cette idée de « brillante » ?

6. La loi n° 2020-766 du 24 juin 2020 [18]

Dite loi « Avia », dont les contours flous laissaient le champ libre à l'interprétation quant à ce que l'on détermine comme « propos haineux ».

Projet de loi, heureusement censuré par le Conseil d'État le 18 juin 2020, du fait de son caractère anticonstitutionnel. Cela laisse néanmoins songeur.

Rappelons que la critique est garante d'un système politique pluraliste, cela ne constitue en rien un acte haineux. Émettre, à travers la critique, la volonté d'améliorer les institutions ne constituant ni volonté de nuire, ni volonté de déstabiliser celles-ci.

7. L'article 3 du Projet de loi d'orientation et programmation du ministère de la justice 2023-2027 [19]

Qui a permis un tour de force, fruit de l'inquiétude de nombreux défenseurs des libertés publiques.

Tout comme pour les régimes autoritaires, tels que la Chine, qui ont de telles pratiques, la France n'a pas à s'enorgueillir d'avoir mis en place de telles mesures. Ces attaques sont intolérables et nous attendons de nos élus qu'ils aient enfin le courage de dénoncer ces agissements et ces projets grotesques.

Ce projet de loi a consacré la possibilité d'activer à tout moment les capteurs suivants de tout appareil connecté jusqu'au sextoy connecté (non ce n'est pas une blague) :

- Caméras
- Microphones
- Matériel de géolocalisation

8. La loi n°2023-380 du 19 mai 2023 portant diverses dispositions autres que la gestion des JO-2024 [20], notamment la Vidéo Surveillance Algorithmique, dites « VSA ».

Encore une fois la démonstration que les « lois d'exception » finissent par entrer dans le droit commun : ce que nous dénonçons fermement :

Cette loi a été présentée aux élus par le biais d'un truchement rhétorique, la définition de la « Démarche d'un individu » : en cherchant à décorréliser les déplacements, démarches, comportements des individus (qui font l'objet de la contestation de la VSA) de la notion de biométrie ; argumentant ainsi que les libertés des français sont ainsi respectées, en l'absence de biométrie des visages. Nouveau « mensonge par omission », étant donné que les seules analyses à la fois de votre silhouette et de votre démarche, suffisent à outrepasser le besoin d'une biométrie des visages.

Le ministère des sports a par ailleurs laissé entendre récemment, dans l'émission Dimanche Politique du 24 Septembre 2023 [21], que cette mesure pourrait être prolongée au-delà de la compétition sportive et au-delà de son statut expérimental.

9. L'Article 7 du projet de loi [22] relatif à la responsabilité pénale et à la sécurité intérieure.

Au Titre III, portant sur l'usage d'aéronefs à des fins d'opérations de sécurité intérieure, lors d'événements divers. Loi présentée sous le sacro-saint argument sécuritaire, qui jusque là a avant tout permis de s'attaquer à toute forme de contestation publique, via l'envoi d'amendes pour des supposés « troubles à l'ordre public » lors de manifestations dites des « casseroles ».

Une nouvelle fois, les instances dirigeantes parviennent à dévoyer l'argument sécuritaire, dans le but d'éviter la contestation toujours plus forte, au regard de la situation de plus en plus catastrophique de la France.



Et le collectif WIKILIBRISTE-COLINU

Peut-on en déduire que toutes ces mesures portent déjà leurs fruits, d'après quelques enquêtes indépendantes menées par des associations, qui luttent contre les dérives autoritaires ?

Nous citons un exemple, qui est le résultat le plus criant :

Affaire dite du 8 décembre 2020 : qui témoigne des fantasmes, d'une hystérisation de la lutte contre les pratiques condamnables, et qui de notre côté inquiète sur les compétences réelles et techniques des services de renseignement.

Services qui dorénavant criminalisent le fait d'avoir des connaissances en informatique comme preuve de l'existence d'« actions conspiratives » [23] - tribune dans Le Monde présente ici [24], et dont quelques clés de compréhension sont données sur la version complète de cette présente lettre ouverte [25].

Dans l'optique de rester concis mais exhaustif, et non partisan, nous tenons à cependant saluer les décisions suivantes prises par la France, conjointement avec l'Union Européenne :

- Harmoniser les standards matériels des câbles d'alimentation pour les appareils électroniques, en positionnant l'USB de type C comme prérequis à la vente d'appareils informatiques sur l'espace commercial européen. Mettant fin par cette réglementation, à la création d'un besoin artificiel via les câbles d'alimentation de type « Lightning ». Pratique imposée à ses clients par l'un des « Géants de la Tech », et qui est à la fois anti-consommateur et anti-concurrentielle.
- Toujours pour cette même marque : contraindre celle-ci à ouvrir son écosystème, en autorisant le téléchargement d'applications à partir de sources extérieures. En effet, la pratique d'un magasin unique d'applications, soumis à une licence de développeur à 100€ par an représente une somme considérable pour les développeurs indépendants. Ainsi que les 30% de commissions supplémentaires, imposées sur les achats intégrés aux applications diffusées via le magasin officiel, qui rongent les marges desdits développeurs indépendants. Mettre un terme à cette situation monopolistique facilitera par la même occasion la diffusion d'applications libres et open source, à ce jour fortement restreintes sur le magasin natif (sauf à ce que ces projets soient soutenus par des fondations, telles que KDE pour n'en citer qu'une).
- Volonté d'amener les constructeurs à proposer à nouveau des batteries amovibles dans tout appareil électronique nécessitant une batterie : proposition qui favorisera la lutte contre l'obsolescence programmée et permettra de meilleures pratiques en matière d'éco-responsabilité.

Notons cependant qu'aucune de ces mesures n'engage la liberté d'expression des citoyens, et visent avant tout la libre concurrence et le marché économique.

Nous tenons également à féliciter les maires qui se sont déjà ancrés localement dans l'adoption de logiciels éthiques à sources ouvertes, montrant ainsi leur soutien au mouvement du logiciel libre et open source. La liste des mairies concernées est disponible ici [26].

Néanmoins, quelques mesures positives ne sauraient annuler une vague de mesures déphasées, décidées en l'absence de concertation, et des experts du domaine, et des français. Cela ne saurait justifier la nature profondément liberticide et anti-républicaine de toutes les lois précédemment mentionnées et celles à venir. Car nous voyons bien ici que l'espace appartenant aux populations, lié à des usages numérisés (« en ligne » comme « hors ligne »), est attaqué de toutes parts et cela s'accélère, faisant fi de toutes les objections de la population et en particulier d'experts des secteurs visés, et au nom du sempiternelle risque terroriste ou criminel. Rappelons un adage :

« si je veux faire piquer mon chien, je dis qu'il a la rage »

Ce qui est sûr c'est que la mise en place de ces divers outils, s'ils sont mis en œuvre, ouvrent la voix aux successeurs pour exercer une pression « numérique » sur leurs concitoyens de plus en plus importante, si et quand bon leur semble... L'autoritarisme, qu'il soit matérialisé ou numérique ne serait finalement plus réservé qu'à quelques pays autoritaires, si souvent pointés du doigt.

Au vu de ces attaques contre nos libertés, la France et ses élus ne peuvent plus en aucun cas donner des leçons de démocratie et de défense des libertés à quiconque. Nous ne sommes plus légitimes sur la scène internationale, la France se meurt et la complaisance d'une majeure partie de la classe politique l'y aide bien.

Aussi, nous en appelons au bon sens républicain des élus, s'il en est, et les exhortons à faire barrage à toute mesure de cette nature, au nom de la sauvegarde de l'état de droit, sans lequel liberté d'expression et pluralisme ne sauraient exister.

Avec nos salutations républicaines et fraternelles.



Sources :

- [1] <https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/553.pdf>
- [2] <https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/>
- [3] https://www.ssi.gouv.fr/uploads/2018/04/anssi-guide-admin_securisee_si_v3-0.pdf
- [4] <https://france3-regions.francetvinfo.fr/occitanie/haute-garonne/toulouse/le-probleme-quand-on-ne-maitrise-pas-son-sujet-c-est-que-cela-se-voit-comment-un-hacker-ethique-passe-au-crible-la-loi-sur-internet-2842799.html>
- [5] <https://www.softwaretestinghelp.com/are-vpns-legal-or-illegal/>
- [6] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1514_projet-loi#D_Article_6
- [7] <https://blog.mozilla.org/netpolicy/2023/06/27/francaise-bloquer-sites/>
- [8] <https://foundation.mozilla.org/fr/campaigns/sign-our-petition-to-stop-france-from-forcing-browsers-like-mozillas-firefox-to-censor-websites/>
- [9] <https://www.assemblee-nationale.fr/dyn/16/amendements/1514/ESPNUM/597>
- [10] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc
- [11] <https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act>
- [12] <https://www.april.org/le-cyber-resilience-act-une-epée-de-damocles-sur-le-logiciel-libre>
- [13] <https://cnll.fr/news/cyber-resilience-act-union-europ%C3%A9enne-menace-logiciel-libre/>
- [14] <https://cnll.fr/static/pdf/cra-lettre-ouverte.pdf>
- [15] <https://www.senat.fr/leg/pjl20-672.html>
- [16] <https://www.laquadrature.net/2021/06/15/loi-renseignement-2-refuser-lemballement-securitaire/>
- [17] <https://www.voxpublic.org/Un-courrier-pour-demander-aux-parlementaires-de-ne-pas-adopter-la-loi-anti.html>
- [18] <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970>
- [19] <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047538699/>
- [20] <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974>
- [21] https://www.francetvinfo.fr/replay-magazine/france-3/dimanche-en-politique/dimanche-en-politique-avec-amelie-oudea-castera_6045800.htmlhttps://www.francetvinfo.fr/replay-magazine/france-3/dimanche-en-politique/dimanche-en-politique-avec-amelie-oudea-castera_6045800.html
- [22] <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000043806985/?detailType=CONTENU&detailId=1>
- [23] <https://www.laquadrature.net/2023/06/05/affaire-du-8-decembre-le-chiffrement-des-communications-assimile-a-un-comportement-terroriste/>
- [24] https://www.lemonde.fr/idees/article/2023/06/14/attaches-aux-libertes-fondamentales-dans-l-espace-numerique-nous-defendons-le-droit-au-chiffrement-de-nos-communications_6177673_3232.html
- [25] <https://wikilibriste.fr/fr/lettre-ouverte>
- [26] https://umap.openstreetmap.fr/fr/map/territoire-numerique-libre_171981#6/47.398/6.636
- [27] <https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789>

Sources subsidiaires :

- Lettre de recommandations du 3 Mars 2022 aux parlement européen, co-signée par **une vingtaine de chercheurs européens**, proposant d'amender le projet sur l'identité numérique eIDAS :
https://www.eff.org/files/2022/03/02/eidas_cybersecurity_community_open_letter_1_1.pdf
- Lettre ouverte publiée le 3 Novembre 2023 et co-signée par **412 scientifiques de 33 pays d'Europe** dénonçant les dérives de la loi européenne sur l'identité numérique (eIDAS) :
<https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr>