Collectif WIKILIBRISTE-COLINU

<u>Objet</u> : Les motivations de notre lettre ouverte

Comme bon nombre de lettres ouvertes, celle à suivre s'adresse aux décideurs : c'est à dire les élus de la république... mais aussi et surtout les français grâce au relais médiatique.

Tout d'abord, les décisions relatives au numérique ne semblent souvent pas avoir la primauté des français, de par l'apparence technique de ce milieu, et les préoccupations telles que le pouvoir d'achat comme priorité immédiate. Ce qui est totalement compréhensible.

Pour autant, les décisions **<u>politiques</u>** relatives à ce secteur ne devraient pas être négligées, au vu du choix dual qui s'offre à nous et à l'heure de l'explosion du numérique : une société informatisée, garante des libertés ? **<u>Ou</u>** un carcan numérique, imposé via des principes, initialement nobles, mais au final dévoyés ?

Aussi, le but de cette lettre est de comprendre les enjeux liés à l'accélération du numérique, son élargissement dans tous les pans de la société, ainsi que de la « techno-surveillance », tels que mise sur le devant de la scène par des élus. Comprendre surtout les enjeux, en lien avec les libertés publiques et le respect des intérêts collectifs des citoyens français, valeurs inaliénables. Une compréhension que nous espérons être le moteur du changement.

Afin de proposer une vue impartiale, nous nous basons sur nos compétences techniques en tant que professionnels du secteur. Compétences que nous mettons en rapport avec notre attachement au respect des valeurs précédemment citées, ainsi qu'à l'éthique, pour présenter à la fois :

- les progrès réalisés dans le domaine, lorsque c'est le cas (voir décisions de l'UE valorisées en fin de lettre)
- les décisions que nous estimons être des régressions à l'encontre des droits élémentaires des citoyens (une majeure partie de cette lettre ouverte, bien malheureusement), voire un changement de paradigme contraire à tout ce contre quoi nos ancêtres se sont battus afin de nous offrir une société libre.

Sur ce dernier point, voici un avant-goût de ce que vous vous apprêtez à (re-)découvrir. Ces risques sont tous détaillés dans la lettre à suivre, et liés :

- Au **<u>durcissement de la surveillance de masse</u>**, en tous lieux, que l'on soit hors ligne comme en ligne - via drones, porte-feuille d'identité numérique, et intrusion dans l'intimité des français au travers de leurs appareils connectés : **amendement n°CS597 du projet de loi 1514, loi n° 2021-998 du 30 juillet 2021**, **article 3 du Projet de loi d'orientation et programmation du ministère de la justice 2023-2027, loi n°2023-380 du 19 mai 2023, Article 7 de la loi n° 2022-52 du 24 janvier 2022**
- À l'entrave (directe ou indirecte) faite à l'émancipation numérique des populations : **<u>criminalisation d'applications utilisant des technologies qui renforcent la protection des utilisateurs,</u>** **<u>ostracisation</u>** **<u>des technologies libres et open source</u>**, **<u>ainsi que la sécurisation des données</u>** (chiffrement, détaillé dans la lettre) : **« Cyber Resilience Act », Affaire dite du 8 décembre 2020**
- A **<u>la censure</u>** : celle directement au cœur des navigateurs internet, des réseaux sociaux, la volonté d'interdire les outils de protection de la vie privée, fragilisant par la même occasion, sécurité en ligne et liberté d'opinions : **tentative d'amendement n°CS553 au Projet de loi n°1514, Article 6 du Projet de loi n°1514 ; loi n° 2020-766 du 24 juin 2020, dite loi « Avia »**

Enfin, connaître l'étendue des mesures qui ont été ou vont être prises permet d'avoir la conscience nécessaire à la mise en place d'actions pour appréhender voire contrer les pièges qui se trament. Le savoir est le pouvoir, et nous voulons savoir nos concitoyens puissants face aux dérives que nous constatons année après année.

Pour un numérique éthique, respectueux des droits humains et des intérêts de ses utilisateurs.

Librement vôtre,

Objet : Lettre ouverte 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 certains représentants en Europe, tentent de proposer des projets de lois visant à élargir le « contrôle numérique » et restreindre les libertés fondamentales inhérentes.

A ce titre, nous listons les mesures les plus récentes dans ce qui suit :

– 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 visiblement montre l'incapacité des élus impliqués à comprendre les ressorts de certains pans du numérique et de sa sécurité. Manque de compétences qui ne peut être pallié qu'en consultant les spécialistes du domaine issus de la société civile, sur des sujets si techniques, sensibles et avec un impact sur la liberté d'expression. En l'occurrence ici le sujet du « VPN » ou RPV (Réseau Privé Virtuel), outil à priori visé par l'amendement, et bien au delà de ce qu'il prétend être réduit aux simples réseaux sociaux.

  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** (e-réputation 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 »**.**

  Aussi, depuis l'essor du télétravail, cette proposition d'amendement est tout bonnement irréaliste : l'ANSSI a par ailleurs fait des 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. Les élus cherchent-ils à fragiliser l'économie numérique, ainsi que l'administration française ?

  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 ». En effet, les RPV sont également utilisés par certains particuliers afin de sécuriser leurs échanges (lorsqu'ils consultent leurs réseaux sociaux sur des wifi publics par exemple) afin de réduire le risque d'attaques sur leur vie numérique, contribuant à éviter entre autres vol de leurs données personnelles (photos de vacances, vidéos personnelles, documents administratifs...) et usurpations d'identité, parmi les différentes menaces en ligne. Il existe une autre façon d'utiliser un RPV pour les particuliers, en passant par un mandataire tiers qui propose d'héberger le service et qui facilite donc grandement son utilisation.

  Enfin, voici, à ce jour, pour information, la liste des pays qui appliquent un blocage ou une restriction sur cet 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 les RPV serait non seulement une énième « usine à gaz », mais également **une renonciation aux principes républicains qui nous différencient de ces régimes autoritaires.**

  De plus, si cet amendement se référait réellement uniquement aux réseaux sociaux, il serait inutile d'incriminer les RPV. En effet, les plateformes demandent déjà de décliner une identité à leurs utilisateurs, via un identifiant unique lié à chaque personne physique ou morale : e-mail et/ou numéro de téléphone. Pour citer de nouveau

l'intervention de notre confrère « L'anonymat n'existe pas sur les réseaux sociaux. Depuis de longues années, les forces de l'ordre sont capables de retrouver des individus et d'obtenir de nombreux détails sur eux. C'est même leur quotidien. ». En aucun cas cet outil ne devrait être assimilé à des actes criminels.

Une fois encore, les élus pointent du doigt un outil qu'ils ne connaissent pas, alors qu'il s'agirait plutôt de pointer la façon d'utiliser cet outil et par qui il est utilisé, ainsi que de participer voire aider au financement du travail de prévention de nos collectifs et associations qu'il convient de faire, avant tout jugement ou incrimination !

Amendement retiré, ce qui n'empêche pas de montrer la totale déconnexion de nombreux élus avec leur population et l'économie de leur pays.

– 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 sites internet figurant sur une liste fournie par le gouvernement, et annoncés comme étant liés à de la fraude en ligne.

  Sachant qu'il existe d'autres mécanismes afin de pallier ce problème, tels que décrits dans la section « De meilleures solutions existent » du billet du 27 juin 2023 du blog de la fondation Mozilla [7]. Et 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. Rappelons que la fondation Mozilla fait preuve de 25 années d'expérience dans le domaine, et a su se hisser à la deuxième place des navigateurs internet les plus utilisés au monde. Ils ont su faire la démonstration d'un modèle alliant hauts standards de sécurité et respect de la vie privée, ce qui légitime leur expertise sur de telles questions.

  Une pétition est à ce titre en ligne [8] ; pétition qui à ce jour est signée par de nombreuses personnes, et personnalités du numérique !

  Même si le sujet a été récemment mis sur la table et en discussion, Nous attendons de nos élus qu'ils s'emparent réellement et rapidement de ce sujet. Et surtout qu'ils consultent et se coordonnent avec les experts des domaines concernés.

– Amendement n°CS597 [9] du projet de loi 1514, visant à sécuriser et réguler l'espace numérique : lier une identité numérique à, **dans un premier temps**, nos actes en ligne sur les réseaux sociaux. Principe, non seulement contraire à l'expression libre, mais également signe de collusion avec des entités privées éloignées de l'intérêt collectif [1]. Intérêts privés, dont l'objectif semble différer de celui avancé : combinée à l'Intelligence Artificielle (IA), aux capacités techniques virtuellement infinies, c'est entre autre la porte ouverte à un retrait quasi-immédiat, en tout lieu de la toile numérique, d'une parole qui ne correspond pas à ce que la majorité présidentielle du moment en attendrait : la fin de toute opposition politique pour un parti en place. L'expression publique sur internet, par les partis d'opposition, s'en trouverait ainsi également menacée, impactant considérablement l'intérêt collectif.

  D'ailleurs, vu les objectifs avancés en termes d'« accélération de [son] adoption » : questionnons l'élargissement de l'identité numérique à l'espace réel **dans un second temps**, via la « e-carte d'identité », stockée dans des applications tierces dites de « portefeuille numérique [2] »; applications qui sont tenues par des entités privées. Des entités qui au passage n'ont pas investi tant d'énergie dans le développement des ces outils dans un but purement altruiste et démocratique : l'identité numérique permettra de collecter une trace constante de l'intégralité de nos interactions, en tout lieu. Une méthode similaire aux identifiants des grandes firmes américaines, exploités par ces « Géants de la tech », dans un rapport de force déséquilibré avec le citoyen, et en lien étroit avec les courtiers en données. Nous serions ainsi transformés en « smartphones humains », et cela serait l'occasion d'atteintes multiples, constantes et en temps réel : au secret médical, à la liberté de circuler, à la liberté d'opinions, à la liberté de s'autodéterminer, entre autres...

  Concernant l'identité numérique comme pré-requis à toute authentification en ligne : à ce jour, il est possible de briser la chaîne du pistage publicitaire en ligne en utilisant des identités multiples selon les réseaux sociaux ;

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 » ?

ce qui participe de la protection de la vie privée numérique de chacun, et non d'une quelconque volonté criminelle. Comme nous le rappelons plus loin, l'anonymat n'existe pas en ligne. Et le pseudonymat peut être brisé si besoin, par les moyens techniques actuels, dans le contexte d'enquêtes de police et uniquement d'enquêtes de police légitimement diligentées, dans le cadre juridique en vigueur. Raison pour laquelle nous dénonçons cette notion de « pré-crime » : une zone d'exception, faite de présomptions et de contrôle.

Par ailleurs, sécurité n'étant pas respect de la vie privée ni anonymat, la sécurisation cryptographique avancée pour cette identité numérique est un tour de passe-passe. Tour de passe-passe rhétorique qui en retire la portée éthique, et dont nous pouvons faire le parallèle avec les acteurs actuels américains, qui chiffrent (sécurisent) effectivement en chemin les données qu'ils nous soustraient, et pour autant, cela n'en retire pas l'emprise qu'ils ont sur nos vies, ni le rapport unilatéral qui est établi.

Entendons donc 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 filatures dans le cadre d'enquêtes criminelles, légitimes et non politisées, 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] qu'il a remis aux représentants des Nations Unies**. Ce qui n'a rien à voir avec la **caricature** d'anonymat à des fins malveillantes proposée par cet amendement. 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 questions et devrait faire l'objet d'un veto catégorique de la part de la classe politique, ou en tout cas de ceux qui prétendent protéger les libertés individuelles de leurs concitoyens. 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.

Retirer cet amendement empêcherait ce genre de scénario. Sur la base des informations ci-présentes, que nous souhaitons loyales et transparentes, questionner les français par voie de référendum sur leur souhait ou non d'adopter cette mesure serait également une démarche politique louable.

– Les attaques successives non seulement du gouvernement français actuel sur les outils à sources ouvertes (open source), 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].

  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 parfois 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.

  Ces attaques sont intolérables et nous attendons de nos élus qu'ils aient enfin le courage de dénoncer ces agissements et ces projets grotesques.

– La loi n° 2021-998 du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement [15], dénoncée de toutes parts comme par exemple [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.

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 ? 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 » [18] - tribune dans Le Monde présente ici [19].

Nous tentons de vous donner quelques clés de compréhension sur l'état de connaissance actuel des personnes censées nous protéger :

1. Le « **cryptage** » est un abus de langage ici et une erreur de débutant dans le monde de la protection des données. Il s'agit ici plutôt de parler de « chiffrement »... D'ailleurs le cryptage n'aurait aucun sens, car cela induirait la non connaissance de l'élément pour décoder la donnée !

2. Le système « **Thor** » n'existe pas. Thor (avec un h – mythologie nordique) serait plutôt « *Tor* » (sans h – informatique) pour « The Onion Router ». En ce qui concerne l'application « **Orboot** », celle-ci n'existe pas à notre connaissance ; par contre, « *Orbot* », oui...

3. Il y a un système d'exploitation ouvert (une « distribution GNU/Linux » précisément) qui s'appelle « TailsOS », et qui effectivement fonctionne sur la mémoire vive d'un ordinateur. Cet outil permet de dénoncer entre autres des scandales d'État, en sécurisant journalistes, avocats et lanceurs d'alerte.
   Mais surtout, il peut s'agir également de moyen de protection pour des personnes ayant un « modèle de menaces en ligne » élevé : comme par exemple des personnes qui travaillent dans sur des projets numériques gouvernementaux, ou sur des projets critiques (que ce soit pour des « Organisme d'Intérêts Vitaux » ou des projets à forts enjeux nationaux) et qui craignent une intrusion dans leur vie numérique, aux conséquences dommageables.
   En revanche, TailsOS ne fonctionne pas avec les processeurs mobiles dits « ARM » : on ne peut donc pas charger ce système sur un smartphone comme il a pu être écrit par ces services !

4. Le système nommé « /e/OS » est un système d'exploitation pour smartphone, basé sur Android (Google). Il n'est en aucun cas un système créé pour la « clandestinité ». Ce système d'exploitation tente de limiter la télémétrie et la revente massive des données personnelles [21], puisque la législation est bien timide pour protéger les données personnelles des concitoyens. Ce système d'exploitation est le fruit d'une organisation à but non lucratif, organisation reconnue association loi 1901 par l'État français depuis avril 2018 [22] ; son développement a pignon sur rue et n'est pas issu d'un recoin sombre du web anonyme. La fondation à son origine n'a jamais cautionné ni soutenu une quelconque activité séditieuse, et devrait faire l'objet de fierté nationale, au vu de l'aspect innovant du projet porté par son fondateur.

5. L'application Signal et toutes les solutions citées sont des logiciels **grand public**, facilement accessibles, et qui n'ont pas besoin d'être téléchargés dans des recoins obscurs de l'internet. Signal est d'ailleurs recommandé pour certains agents du service public, au même titre qu'Olvid. Ces agents du service public se caractériseraient-ils « tous par leur culte du secret et l'obsession d'une discrétion tant dans leurs échanges, que dans leurs navigations sur internet » ? Si oui, pourquoi ne pas leur apporter le même traitement ?

Pour rappel, le chiffrement sert à protéger les données, qu'elles soient en transit sur un réseau ou stockées sur un disque dur, protégé du vol physique ou virtuel. Se protéger des attaques de plus en plus sophistiquées de réels criminels numériques ne fait pas de la personne un séditieux ou un criminel !

Cette affaire est très grave et montre deux choses :
(i) que notre service de renseignement français DGSI n'est pas à la hauteur des enjeux dans ce monde numérique, qu'il aura du mal à protéger nos compatriotes avec ce niveau, et qu'il est temps qu'ils reçoivent une formation adéquate et solide en cybersécurité.
(ii) qu'il est tout à fait possible pour des personnes avec un certain pouvoir de dévoyer les lois. Lois mises en place au départ pour protéger les citoyens, mais qui au final desservent lesdits citoyens, bien plus que les réels criminels et terroristes.

Dans la même lignée, qui témoigne toujours d'une hystérisation de la part des pouvoirs publics :

– La loi n° 2020-766 du 24 juin 2020 [23], dite loi « Avia », dont les contours flous laissaient champ libre à l'interprétation quant à ce que l'on détermine comme « propos haineux ». 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.

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

– L'article 3 du Projet de loi d'orientation et programmation du ministère de la justice 2023-2027 [24], qui a permis un tour de force, fruit de l'inquiétude de nombreux défenseurs des libertés publiques. Projet de loi qui 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

  De même qu' avec l'identité numérique en ligne, pouvons-nous nous attendre aux mêmes dérives politiques, par les voies officieuses, que celles citées ci-haut ?

  Tout comme pour les régimes dictatoriaux, 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.

– La loi n°2023-380 du 19 mai 2023 portant diverses dispositions autres que la gestion des JO-2024 [25], notamment la Vidéo Surveillance Algorithmique, dites « VSA ». Loi présentée aux élus par le biais d'un truchement rhétorique, que nous détaillons : est considérée comme biométrie, toute collecte, mesure et analyse (« -métrie ») de l'un des éléments suivants, propres à la condition d'un être vivant (« bio- »), à fin d'en déterminer l'unicité au travers de ses attraits distincts : entre autres parmi les éléments les plus connus :

  - Caractéristiques physiques par le biais d'une prise d'empreinte de tout ou partie du visage, des yeux (iris), ou même des mains (paumes) ou des doigts (empreintes digitales).
  - Démarche d'un individu.

  Et c'est sur ce dernier point qu'est intervenu le truchement du débat : en cherchant à décorréler 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 [26], que cette mesure pourrait être prolongée au-delà de la compétition sportive et au-delà de son statut expérimental.

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

– L'Article 7 du projet de loi portant sur l'usage d'aéronefs à des fins d'opérations de sécurité intérieure [27], 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 « casserolades ».

  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.

Toujours dans l'optique d'apporter notre contribution du point de vue technique, et afin de montrer notre impartialité, nous tenons à 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 [28].

—

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. 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 toute objection ou remarques de la population et en particulier d'experts des secteurs visés, et au nom du sempiternelle risque terroriste ou criminel. Sur ce sempiternel risque avancé comme argument, 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 à vos 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 – nombre de projets de loi du même acabit restant probablement à venir – n'est finalement plus réservé qu'à quelques pays, 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 à votre bon sens républicain, s'il en est, et vous 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.

Madame, Monsieur, nous vous prions d'accepter nos salutations républicaines et fraternelles.

Extrait du Préambule de la Constitution Française de 1789 :

> *Les représentants du peuple français, constitués en Assemblée nationale, considérant que l'ignorance, l'oubli ou le mépris des droits de l'homme sont les seules causes des malheurs publics et de la corruption des gouvernements* [...] [29]

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-epee-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.laquadrature.net/2023/06/05/affaire-du-8-decembre-le-chiffrement-des-communications-assimile-a-un-comportement-terroriste/

[19] 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

[20] https://www.allocine.fr/film/fichefilm_gen_cfilm=129477.html

[21] https://e.foundation/fr/about-e/

[22] https://www.societe.com/societe/e-foundation-840146336.html

[23] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970

[24] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047538699/

[25] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974

[26] 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

[27] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000043806985/?detailType=CONTENU&detailId=1

[28] https://umap.openstreetmap.fr/fr/map/territoire-numerique-libre_171981#6/47.398/6.636

[29] https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789