Fédération des fournisseurs d'accès à Internet associatifs
(dite « Fédération FDN »)
FFDN — 16, rue de Cachy — 80 090 Amiens
Déclarée en préfecture de la Somme — W751210904

Réponse à la consultation de l'ARCEP « Smartphones, tablettes, assistants vocaux. . .Les terminaux sont-ils le maillon faible de l'ouverture d'Internet ? »

Fédération FDN

11 janvier 2018

1 Introduction

1.1 Présentation

La présente réponse est rédigée à six mains, par trois associations partenaires : La Quadrature du Net, la Fédération FDN et Exodus Privacy. Les deux premières associations travaillent ensemble sur plusieurs dossiers, en particulier l'étude du Code des Communications Electroniques européen. La troisième vient de se créer.

Pour rappel, La Quadrature du Net est une organisation de défense des droits et libertés fondamentales à l'ère du numérique qui agit, tant au niveau national en France, qu'au niveau européen, et ce depuis 2008. Ses activités sont concentrées sur l'implication des citoyens dans la défense de leurs droits et libertés. L'organisation produit des analyses de textes juridiques, aide les citoyens à les comprendre, et développe des outils pour aider les citoyens à agir, par exemple, en assurant le suivi des votes exprimés par les députés européens.

La Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN, créée en 2011, regroupe, quant à elle, des fournisseurs d'accès à Internet ayant la forme d'associations sans but lucratif, régies par le droit local correspondant (lois de 1901 et 1905 en France, lois similaires dans d'autres pays). Elle rassemble aujourd'hui 26 opérateurs : 25 en France (métropolitaine et outre-mer) et un en Belgique, dont certains comptent parmi les plus anciens fournisseurs d'accès à Internet encore en activité en France. Notre fédération est constituée autour de principes forts, comme la défense et la promotion de la neutralité du Net, et pas uniquement sur une communauté de structure juridique. Les fournisseurs d'accès que nous représentons sont tous animés par des utilisateurs bénévoles du réseau. La diversité des acteurs rassemblés nourrit une expérience de terrain riche, qui lui donne un point de vue particulier dans le cadre de cette consultation : nos associations sont placées juste à la jonction entre le monde des utilisateurs finals et celui des opérateurs : nous voyons l'endroit et l'envers du décor.

Exodus Privacy est une association loi 1901 animée par des hacktivistes. Elle développe une plateforme (nommée εxodus) d'analyse du respect de l'intimité et de la vie privée par les applications Android. Cette plateforme met à disposition du public des rapports listant, entre autres, les mouchards embarqués dans les applications Android.

1.2 Remarques générales

Pour commencer, nous aimerions encourager la direction prise par l'ARCEP sur ce dossier : le sujet des terminaux est capital et les enjeux sont de taille. Lesdits enjeux sont, dans l'ensemble (en ce qui concerne ce document comme le pré-rapport qui lui précède) bien compris. C'est une bonne base de travail, qu'il faut consolider.

Cependant, les problèmes abordés débordent largement de ce que que nous pouvons apporter comme éléments dans la réponse à la présente consultation –et dans les délais impartis. Il faut que le régulateur développe des connaissances en interne sur le sujet. Pour cela, nous nous tenons à la disposition du service Internet et Utilisateurs pour l'aiguiller dans ses recherches.

Enfin, nous avons noté, dans la formulation de certaines questions, que l'ARCEP accepte sans les remettre en question des présupposés qui viennent de l'industrie. Attention : s'il doit écouter tous les acteurs du marché, nous conseillons au régulateur de tenir une position critique vis-à-vis d'eux et de ne pas reprendre tels quels les termes métiers employés par les commerciaux sans avoir pesé avec précaution ce qu'ils impliquaient. L'ARCEP n'a rien à vendre, elle s'intéresse à l'intérêt général.

Le régulateur remarquera que les réponses à ses questions sont liées entre elles, et se basent sur les mêmes grands principes, qui viennent rythmer ce document. Parmi ceux-ci, nous tenons à insister tout particulièrement sur la nécessité, ici, de faire *toujours* valoir le **contrôle de l'utilisateur final** sur le terminal. C'est ce contrôle qui garantit que les droits fondamentaux essentiel de l'utilisateur sont conservés en pratique : s'il n'est pas position de contrôle vis à vis de son terminial, on nie à l'utilisateur la responsabilité qui fonde ses droits fondamentaux en tant que citoyen.

Ce contrôle doit s'exercer autant sur le terminal lui-même que sur la manière dont le terminal fait transiter des données : aussi, nous sommes en faveur d'un strict respect du règlement général sur la protection des données (RGPD) et des lignes directrices du G29 pour ce qui est du traitement de données personnelles.

Aucune partie de ce document n'est soumise au secret des affaires.

2 Thème 1 : Quel serait le mode idéal de mise à disposition de services et de contenus en ligne ?

2.1 Question n° 1.

Entre applications et sites Internet, quelles possibilités ?
Quelles différences entre ces modalités de mise à disposition des contenus ?
Quelle est la préférence des utilisateurs ? Cela diffère-t-il selon les équipements terminaux ?

Il est difficile pour nous de répondre à la question sur la « préférence des utilisateurs » : les fournisseurs d'accès à Internet de la Fédération FDN ne pistent pas leurs abonnés.

Au delà de la potentielle valeur ajoutée des applications mobiles pour les utilisateurs finals, nous attirons l'attention du régulateur sur leur effet particulièrement inquiétant sur la liberté d'accès aux contenus sur le web. En effet, en fragmentant les usages (à un besoin correspond une application, c'est le sens du fameux « there's an app for that »), l'utilisateur, au lieu d'être face à un navigateur qui lui ouvre la porte vers tous les contenus disponibles, se retrouve tributaire, pour accéder à un contenu ou un service, d'une part des systèmes d'exploitations majoritaires (cf. notre réponse à la question n° 5), d'autre part des décisions déjà très arbitraires des magasins d'applications et de leurs politiques éditoriales. Cela laisse bien peu de garanties pour faire respecter un droit pourtant fondamental (et maintenant garanti par les textes européens) de l'utilisateur final.

Nous aurions donc tendance, pour cette raison, à préférer l'accès aux contenus par le biais d'un navigateur web, qui lui, ne limite en aucune manière quel site doit s'afficher ou non.

De plus, les capacités des navigateurs augmentent sans cesse et permettent des usages de plus en plus riches et de plus en plus intégrés avec le système d'exploitation. Il est ainsi désormais possible d'accéder au positionnement de l'appareil, à sa caméra, à son micro ...Ceci combiné à la possibilité de toucher une grande partie des systèmes sans devoir gérer les spécificités de chaque système d'exploitation, ni d'avoir à passer par l'éventuel magasin d'application spécifique de l'éditeur de celui-ci et ses règles contraignantes, rendent le développement de sites Internet plutôt que d'applications de plus en plus attrayants.

Mais il ne faut pas oublier que les navigateurs web, en s'ouvrant à des usages applicatifs, ont aujourd'hui accès à des éléments critiques des terminaux, rendant ces derniers vulnérables dans certains cas [1]. Il ne faut pas habiller Pierre en déshabillant Paul : permettre à l'utilisateur final d'être moins enfermé dans les logiques de fragmentation des usages ne doit *pas* se faire au détriment de sa sécurité et de sa vie privée.

1. C'est ainsi que certains sites peuvent tracer les utilisateurs à leur insu en utilisant l'accès donné au navigateur à l'accéléromètre du téléphone : `http://web.engr.illinois.edu/~caesar/papers/tracking-ndss16.pdf`

Il faut donc veiller d'une part à ce que les standards ouverts qui permettent au web aujourd'hui de se poser en alternative sérieuse face aux applications mobiles doivent faire l'objet d'une veille attentive constante. Le W3C, qui les établit, a déjà intégré les DRM dans ces derniers [2]. Tout laisse à penser que le choix du web doit s'associer à un réel souci –au sens fort– pour les standards ouverts. D'autre part, notamment en ce qui concerne les autorisations à fournir au navigateur pour accéder à tel ou tel élément (caméra, accéléromètre, clavier ...), tout doit être sous le contrôle de l'utilisateur final. Naturellement, ce dernier doit être mieux informé pour que ce contrôle ne se résume pas à cliquer « oui » comme on clique « oui » sur la bannière « j'accepte les cookies sur ce site web ».

A ce propos, remarquons qu'installer une application mobile amène souvent à la laisser accéder à de nombreuses données et fonctionnalités du terminal –sans que cela soit pas ailleurs tout à fait justifié par l'éditeur de l'application en question. Des applications d'espionnage déguisées, afin d'appâter les victimes, en jeux gratuits, en application de messagerie chiffrée ou bien en antivirus sont ainsi installées par des millions d'utilisateurs. [3] [4].

Au contraire, les navigateurs ont aujourd'hui des politiques de sécurité clairement définies, compréhensibles et efficaces ; ils évitent la plupart de ces problèmes (bien que ce ne soit pas parfait, cf. l'exemple que nous citons plus haut). On pourrait imaginer, pour améliorer ce contrôle de l'utilisateur, une gestion plus fine de ces autorisations, où l'utilisateur pourrait choisir à quel niveau il souhaite que son terminal ou son navigateur le sollicite pour lui demander de contrôler ce à quoi il accède (« je veux être alerté quand une application demande l'accès à mon accéléromètre : oui/non », par exemple), ou par liste blanche en fonction de la confiance accordée au site ou au service : « le site lemonde.fr a le droit, mais pas les autres ». Ce type de paramétrage aurait l'avantage de donner aux utilisateurs les plus informés la possibilité de contrôler les accès de manière fine sans forcément noyer les utilisateurs qui n'en auraient pas besoin sous les messages d'alerte. Il ne faut pas réduire les droits des utilisateurs sous prétexte qu'on les ennuie : qu'une grande part des utilisateurs ne touche jamais à cela n'est pas un problème. Qu'une fois informé, l'utilisateur ne puisse rien faire, c'en est un.

2.2 Question n° 2.

Dans quelle mesure les développeurs doivent-ils adapter leurs applications selon le type de terminal, de navigateur ou de magasin d'applications utilisé ?

Dans le cas d'une application native, les développeurs sont soumis aux contraintes spécifiques à chaque plateforme (procédures de développement, langage de programmation, bibliothèque de code partagée par le système, etc.) : ainsi, il faudra produire (et maintenir) un binaire différent pour iOS et pour Android.

Dans le cas des terminaux fonctionnant sur Android qui sont tous différents, il faudra

2. [https://www.eff.org/deeplinks/2017/07/amid-unprecedented-controversy-w3c-greenlights-drm-web
3. http://www.zdnet.com/article/android-app-stores-flooded-with-1000-spyware-apps/
4. http://www.securityweek.com/hundreds-fake-android-antivirus-apps-deliver-malware

peut-être vérifier la compatibilité de l'application avec les principaux terminaux sur le marché.

Dans le cas d'un site web, si les standards du W3C permettent de mettre au point des sites Web relativement interopérables quel que soit le navigateur et le terminal, le développeur effectue toujours des adaptations pour parfaire cette interopérabilité, car la manière dont les standards sont implémentés diffère légèrement d'un navigateur à l'autre : ainsi, on modifiera les règles de style (CSS) pour permettre à Internet Explorer de produire le résultat attendu. Pour s'adapter à la plupart des terminaux (mobiles et fixes, quelle que soit la résolution), les développeurs web utilisent aujourd'hui des outils qui pemettent aux sites de s'adapter à l'écran du terminal de l'utilisateur qui le visite. On appelle cela rendre un site *responsive.*. Cela présente l'avantage, pour le développeur, de n'avoir à maintenir qu'un seul site web. L'alternative à cette technique, maintenant largement répandue, mais ayant l'inconvénient d'alourdir un peu le chargement des pages web, est de proposer, en marge du site web principal, optimisé pour les tailles d'écran larges d'ordinateurs fixes, un « site mobil », dont les fonctionnalités sont souvent plus limitées que le premier, optimisé pour l'affichage sur un téléphone, par exemple. Cette méthode oblige à maintenir, du point de vue éditorial comme du point de vue du code, deux sites au lieu d'un seul.

2.3 Question n° 3.

Est-ce possible pour un fournisseur de contenus de présenter son offre sur toutes les versions d'un terminal ? A quel coût (technique, financier, etc.) ?

Nous pouvons aujourd'hui constater qu'un site web créé dans les années 90 reste aisément lisible de nos jours alors qu'une application de la même époque est particulièrement difficile à installer et à exécuter. Cette différence s'explique par l'absence de code exécutable dans les sites web : décoder et afficher du texte ou une image sont des tâches simples comparées à celle de faire fonctionner une application entière de manière fiable et sure. Il est intéressant de noter que les sites web qui s'étaient appuyés sur des technologies telles que Macromedia Flash, et son plug-in navigateur, ne sont en revanche presque plus accessibles. Ainsi, la meilleure compatibilité entre terminaux, quels qu'ils soient, est obtenue en maintenant séparés contenus et affichage de ceux-ci . Les formats des données évoluent lentement au regard de l'évolution des terminaux.

Nous n'aborderons ici que la réponse à cette question du point de vue des sites webs et « progressive web apps » . En effet, les applications mobiles, pour être diffusées sur les deux principaux magasins d'applications, demandent un coût non négligeable –nous y revenons dans la réponse à la question suivante. aussi il n'est pas rare qu'une application présente sur une plateforme ne le soit pas sur la deuxième. Aussi, ces technologies viellissent mal : une application développée pour iOS 5 ne sera pas forcément exécutable sous iOS 6. Au final, nous considérons que pour présenter une offre de contenus au plus large public, le web semble mieux indiqué.

La principale difficulté à présenter un contenu au travers d'un site web est l'utilisation de technologies non disponibles ou non encore disponibles sur certaines plateformes.

Cependant, les navigateurs offrent de plus en plus de possibilités et cette difficulté tend à disparaître bien qu'elle soit encore présente. L'éditeur du système d'exploitation du terminal mobile joue souvent un rôle primordial sur la disponibilité d'un navigateur récent.

Le cas des « Service Workers » est particulièrement intéressant. Ceux-ci sont définis comme « [A] method that enables applications to take advantage of persistent background processing, including hooks to enable bootstrapping of web applications while offline. » [5]. Cette technologie fait disparaître une part importante des avantages usuellement avancés en faveur des applications par rapport aux sites web. Néanmoins, en pratique, son utilisation est bloquée car Safari, le navigateur sur Apple iOS (y compris lorsque l'utilisateur pense utiliser un autre navigateur) ne fournit toujours pas cette fonctionnalité que personne ne déploierait un site web qui ne fonctionne pas sur iOS.

Cela doit évoluer avec la prochaine version de Safari [6] mais il est important de noter le retard de Safari sur les autres navigateurs. Le site `https://caniuse.com` permet de suivre les évolutions dans le temps des fonctionnalités des navigateurs grâce à son affichage « Date Relative » ; la compatibilité des navigateurs avec la technologie des Service Workers est visible sur la page `https://caniuse.com/#feat=serviceworkers`.
Au vu des moyens d'Apple, il est difficile de penser que la non-implémentation de cette technologie pendant des années n'a obéit qu'à des contraintes financières ou techniques. Cela est d'autant plus intriguant lorsque l'on considère les Service Workers comme une technologie qui permet à de nombreux éditeurs d'applications iOS de ne pas passer par l'AppStore et ses contraintes, mais au contraire de laisser les utilisateurs finals accéder directement à leur site web. Le site `https://web.archive.org/web/20171228020446/https://jakearchibald.github.io/isserviceworkerready/` indique aussi la prise en charge de cette technologie par les navigateurs et montre à nouveau le retard frappant d'Apple et de son navigateur.

Ainsi, grâce à des limitations techniques (manque de fonctionnalités du navigateur intégré) et des règles pour la publication dans son magasin d'applications (interdiction de publier d'autres navigateurs en pratique), un éditeur de système d'exploitation peut, empêcher les éditeurs de passer par le web pour présenter leurs offres aux utilisateurs, ce qui présente un frein majeur à la diffusion la plus large possible de contenus.

Pour ce qui est des coûts amenés par la compatibilité entre versions d'un terminal mais aussi entre terminaux, il faut mettre en regard plusieurs éléments : part de marché des équipements, revenu moyen par utilisateur pour chaque équipement, puissance de calcul des équipements, âge et choix techniques et politiques de l'éditeur du système d'exploitation. Les coûts ne peuvent être étudiés qu'en fonction des revenus qui peuvent être escomptés. L'ARCEP est déjà habituée à la plupart de ces éléments et nous avons exposé ci-dessus les contraintes amenées par les choix techniques et politiques des éditeurs de systèmes d'exploitation ; l'âge des équipements n'est quant à lui qu'un multiplicateur de ces contraintes.

5. `https://w3c.github.io/ServiceWorker/`
6. `https://webkit.org/blog/8042/release-notes-for-safari-technology-preview-46/`

2.4 Question n° 4.

Pour les développeurs, quels sont les avantages et les inconvénients des différentes modalités de mise à disposition de leur offre (sécurité, conditions de partage des données de consommation et de consultation, modalités de tarification, visibilité, etc.) ?

En ce qui concerne la sécurité, quel que soit le mode d'accès au service, il est absolument nécessaire de garantir la sécurité du canal de transfert entre le serveur et l'utilisateur final, ainsi que l'intégrité du programme téléchargé. Ce point est donc non-discriminant.

Pour ce qui est de la visibilité et de la facilité de publication et de suivi, les avantages des magasins propriétaires principaux (l'*Apple App Store* et *Google Play Store*) sont régulièrement rappelés : suivi des téléchargements, visibilité accrue, tenue à jour des applications, vérification de l'intégrité de l'application [7], recherches de virus, etc.. Nous ne nous attardons pas là-dessus.

Ces avantages sont contrebalancés par un inconvénient de taille : la publication d'une application dédiée à un OS nécessite de respecter les règles dictées par le magasin d'applications. Chacun d'entre eux ayant ses propres règles, les spécifications de l'application peuvent être soit adaptées aux règles les plus restrictives ou bien être protéiformes. Ainsi, un développeur qui choisit de produire des applications pour telle ou telle plateforme doit se conformer à ses règles, complètement arbitraires, et n'a pas le moindre recours. On peut citer l'exemple de ce groupe de presse, qui a lancé son application pour diffuser ses bandes dessinées, destinée à un public plutôt jeune. La plateforme d'Apple a refusé au début la diffusion de l'application, arguant que certaines bandes dessinées ainsi publiées contenaient de la nudité. On était pourtant très loin de la bande dessinée adulte...Aucun recours possible, les développeurs ont été obligés de faire avec.

Pour le dire autrement, les avantages apportés par le contrôle que les principaux magasins d'applications ont sur ce qu'il s'y diffuse va avec les inconvénients tout à faits malsains de tout système de contrôle fermé : l'abus arbitraire de ce contrôle, prenant ici la forme de la censure de contenus, sans recours judiciaire. Cela peut aller jusqu'à permettre à des gouvernements peu respectueux des droits fondamentaux de profiter de ce contrôle pour censurer des services, comme actuellement en Iran, où l'application Signal, par exemple, est impossible à télécharger sur la plateforme de Google [8]. Les développeurs de Signal, bien évidemment, n'y peuvent rien.

De plus, ce qui est perçu comme des avantages peut se retourner contre le développeur. C'est ainsi que, pour Android ; utiliser les bibliothèques de code de Google – pratiques pour les développeurs pour mieux interagir avec le système d'Android et mises à leur disposition s'ils publient via son magasin d'application– contraint, de fait, la diffusion de l'application sur le *Play Store* en rendant l'application dépendante de ces morceaux de code. L'application Signal, par exemple, a été récemment distribuée, en

7. On s'assure que l'application mise à disposition n'a pas été remplacée par un programme malveillant en vérifiant sa signature unique, délivrée par le développeur.

8. `https://www.theverge.com/2018/1/2/16841292/iran-telegram-block-encryption-protest-google-signal`

sus du magasin de Google, sur le site web de l'éditeur du logiciel [9], afin, notamment de permettre aux utilisateurs d'OS ou de magasins d'applications alternatifs d'installer le programme. En réalité, le programme ainsi diffusé dépend toujours des bibliothèques de Google et est donc très difficle à installer pour quelqu'un qui n'a pas de compte sur le *Play Store*. Autant diffuser via le magasin d'applications à ce compte.
Il est possible de se débarrasser de ces bibliothèques de code, et de les remplacer (quand elles existent) par des alternatives, mais cela demande de revoir tout le code de l'application, ce qui demande un gros investissement en termes de travail, élevant d'autant le coût pour « sortir » du magasin d'applications et la dépendance du développeur à la plateforme.

Dans le cas d'une publication sur le Web, seules les lois en vigueur peuvent contraindre la diffusion de l'application : il n'y a pas d'autre intermédiaire entre le développeur et l'utilisateur final autre que les moyens techniques permettant l'exécution et le transfert de l'application. Ainsi, si une application fait l'objet d'une réquisition, celle-ci est soumise à l'appréciation d'un juge et non d'une entité privée, et le développeur ou l'éditeur du logiciel ont la possibilité de faire un recours. C'est un avantage de taille. De plus, cette manière de diffuser peut permettre une meilleure interopérabilité de l'application, en offrant la possibilité d'atteindre, en même temps, les utilisateurs de plusieurs OS, si le programme délivré ne dépend d'aucun bibliothèque de code contraignante. Certaines choses sont cependant plus difficiles à faire, par exemple garantir l'intégrité du programme téléchargé (on peut proposer à l'utilisateur de vérifier lui-même la signature du programme, mais en pratique seuls les utilisateurs avancés y pensent), et il est plus difficile de s'assurer que l'application est régulièrement mise à jour par les utilisateurs finals, qui doivent régulièrement visiter le site pour télécharger une nouvelle version du programme.

Dans le cas d'une application dédiée, il est facile de la rendre payante, mise à part l'éventuelle commission demandée, en tant qu'éditeur, par le le magasin d'applications. Pour ce qui est de la diffusion sur un site web, cela est également possible ; mais il faudra intégrer des développements liés à la gestion de ce paiement en ligne, qui peuvent s'avérer payants eux aussi (Paypal demande, par exemple, une commission pour le paiement en ligne). La plupart des solutions de paiement en ligne aujourd'hui utilisées sur le web, si elles sont correctement implémentées, perrmettent une sécurité correcte des paiements.

Certains magasins d'applications alternatifs comme *F-Droid* peuvent être vus comme des éléments médians entre ces deux modèles : tout en permettant notamment un suivi simple des mises à jour, le magasin d'application est édité par une organisation à but non lucratif, qui n'a aucun intérêt à imposer des règles similaires à ses concurrents, permettant ainsi au développeur de s'affranchir de cette contrainte.

2.5 Question n° 5.

Y a-t-il de la place pour des magasins d'applications alternatifs ?

9. `https://signal.org/android/apk/`

Les contraintes de publication dans les deux principaux magasins d'applications actuels (*Apple App Store* et *Google Play Store*) créent, pour les utilisateurs, une place pour des alternatives. Il est actuellement possible de citer en exemple *Cydia* sur iOS et *F-Droid* sur Android. Il en existe des dizaines d'autres, en particulier sur Android.

L'utilisation de ceux-ci est assez répandue malgré leur difficulté d'installation, clairement hors de portée d'un utilisateur non informé. En effet, *Cydia* sur iOS nécessite un appareil dit « jailbroken » [10]. Sur Android, installer *F-Droid* requiert de passer par un paramètre avancé dont l'activation est soumise à confirmation avec un message expliquant qu'une application ne provenant pas du *Play Store* peut être néfaste – tandis que le *Play Store* contient lui aussi de nombreuses applications néfastes, de type « spyware ». Ce n'est évidemment pas l'apanage des seuls magasins d'applications alternatifs contrairement à ce que Google insinue.

En parallèle, pour les développeurs, la publication sur chaque magasin d'applications représente un investissement important et la relativement faible utilisation des magasins alternatifs ne rend pas toujours l'opération économiquement rentable. Permettre à la majorité des utilisateurs, généralement peu compétents en ce qui concerne la technique, d'installer ces magasins d'applications, augmenterait l'intérêt de publier des applications sur ceux-ci, ce qui amènerait en retour davantage d'utilisateurs sur les magasins alternatifs et pourrait enclencher un cycle de développement de ceux-ci.

2.6 Question n° 6.

Pour l'accès aux différentes fonctionnalités des équipements terminaux, les développeurs ont-ils suffisamment de garanties ?

Les développeurs sont relativement contraints dans leur travail, contrairement à ce qu'on peut penser de prime abord. Ces contraintes sont principalement techniques et pas toutes du même ordre. Ce qui est intéressant, c'est qu'elles posent des problèmes politiques.

Tout d'abord, les autorisations demandées à l'utilisateur peuvent bloquer l'accès à certaines fonctionnalités du terminal, parce que l'utilisateur l'a décidé : c'est une contrainte avec laquelle il faut composer. On ne peut pas donner par défaut tous les droits aux développeurs sous prétexte que c'est plus pratique. Une application doit pouvoir fonctionner avec le minimum d'autorisations qui lui est nécessaire. Ces autorisations sont aussi extrêmement larges et parfois décorrelées du besoin réel du développeur pour son application : on doit ainsi donner les droits à l'application sur *tout* l'espace de stockage du téléphone alors qu'elle n'aurait par exemple besoin que de contrôler un dossier pour fonctionner. Cette partie peut être affinée.

Ensuite, des aspects dont nous avons déjà parlé reviennent : la version de l'OS ou du navigateur, quand il n'y a pas d'interopérabilité entre les versions, peut être bloquante dans le développement d'une application. De la même manière, la diversité du parc de

10. C'est-à-dire, sur lequel l'utilisateur final a obtenu le contrôle complet du système, cf. `https://fr.wikipedia.org/wiki/Jailbreak_d\%27iOS`

terminaux mobiles peut occasionner l'incompatibilité de certains terminaux qui n'ont pas les ressources nécessaires pour faire fonctionner l'application. L'éditeur de l'OS a, rappelons-le, la possibilité de changer ou de retirer certaines fonctionnalités de l'API qui permet d'exploiter certaines fonctions de l'OS : le développeur est ici dépendant de l'éditeur de l'OS.

Enfin, rappelons que la documentation des terminaux mobiles est extrêmement difficile d'accès. Le travail de Replicant [11] a montré combien il était difficile de bâtir des alternatives à Android, car certains constructeurs ne diffusent aucune documentation technique de leurs équipements, arguant du secret commercial. Les développeurs sont obligés de chercher par eux-mêmes comment fonctionne le composant pour pouvoir l'utiliser. Cela pose un problème immédiat, qui est de ralentir le travail de développeurs d'OS alternatifs, notamment, et un autre problème : il est impossible aujourd'hui de savoir comment fonctionne un smartphone, et donc de garantir à l'utilisateur final qu'il en a la maîtrise complète. Rien ne vient en effet confirmer le fait que la puce du modem, souvent directement reliée au micro du téléphone, ne puisse pas l'écouter à son insu, par exemple. Si l'utilisateur final n'a pas le contrôle total sur la machine, alors ce n'est pas lui qui en est le propriétaire. C'est d'autant plus inquiétant que ce terminal est au centre de la vie intime de l'utilisateur final.

2.7 Question n° 7.

A quels critères peut-on reconnaître une politique éditoriale acceptable ?

La question est vaste, preuve en est la longueur des conditions des magasins d'applications majoritaires [12] [13] [14]. Il est illusoire d'en attendre une réponse simple, et courte, dans le cadre de cette consultation.

Ceci dit, nous allons tout de même noter quelques éléments qui constituent, selon nous, une politique éditoriale inacceptable —mais dont l'absence ne garantit par une politique éditoriale acceptable.

Premièrement, certaines applications sont parfois rejetées sans qu'une raison soit fournie ou bien pour une raison particulièrement floue. Même lorsque des applications finissent par être acceptées dans certains magasins, le délai d'acceptation peut avoir une influence majeure sur sa diffusion : retarder d'uniquement deux ou trois semaines une publication d'application liée à un évènement ponctuel ou à un phénomène « viral » suffit à enlever tout intérêt à ladite application.

Ensuite, il existe des règles exigeant par exemple que les applications proposées sur les magasins d'application fassent preuve d'une certaine originalité. Outre le fait que de tels critères sont flous, les applications seront comparées à ce qui est pré-installé avec le système d'exploitation de l'éditeur, créant un déséquilibre : les applications tierces doivent montrer qu'elles présentent un intérêt supérieur à celles de l'éditeur du magasin

11. https://blog.replicant.us/2017/12/contributions-to-arcep-work-on-terminal-devices-and-public-consultation/
12. https://developer.apple.com/app-store/review/guidelines/
13. https://play.google.com/intl/None/about/developer-content-policy/
14. https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html

d'applications. En d'autres termes, dans le cas d'applications concurrentes aux siennes, l'éditeur du magasin d'applications peut trivialement invoquer un manque d'originalité pour restreindre une diffusion.

D'une manière similaire mais hors de son magasin d'applications, Google restreint l'utilisation de la marque « Android » : il est interdit de remplacer les applications Google par défaut par d'autres. Ainsi, Samsung ne peut configurer une autre application mail par défaut autre que « GMail » sur un équipement et le qualifier de système « Android ».

Il est aussi possible de citer l'interdiction établie par Apple de mentionner d'autres plateformes mobiles ou bien celle de Google de faciliter l'installation d'applications par d'autre moyen que Google Play.

Finalement, nous souhaitons souligner qu'un label ou une charte à laquelle les magasins d'application devraient adhérer ne résoudrait probablement pas le problème, le processus de décision de celles-ci étant particulièrement opaque.

3 Thème n° 2 : Qu'est-ce qui explique les succès et les échecs passés des terminaux et OS ? Quelles questions soulèvent les interfaces de demain ?

3.1 Question n° 8.

Quels sont les changements à l'œvre dans les conditions concurrentielles qui structurent le monde des terminaux et des systèmes d'exploitation ?

Cette question est très vaste. Trop, pour l'échelle de cette consultation.

De plus, la manière dont elle est formulée pose un cadre où quelque chose aurait forcément changé –ce qui n'est pas clair : de manière générale, les logiques qui président au renforcement des oligopoles, que ce soit du côté des terminaux que du côté des systèmes d'exploitation sont les mêmes depuis plusieurs années. Ainsi, nous ne savons pas ce qu'attend le régulateur ici, et ce cadre qui suppose d'emblée que des changements sont à l'œuvre (laissant entendre que ces changements sont connus) nous rend dubitatif, au mieux.

3.2 Question n° 9

Quelle est la place des fournisseurs d'accès à Internet dans l'univers des terminaux ?

Les fournisseurs d'accès à Internet sont un élément essentiel. D'une part, il permettent la connexion des terminaux à Internet. D'autre part, ils permettent aux utilisateurs finals d'accéder aux applications, services et contenus qu'ils recherchent.
C'est pourquoi ils doivent garantir un accès non discriminant aux diverses applications,

contenus, et services. Il est donc impératif de défendre la neutralité de ce réseau. Ceci, afin de garantir les droits et libertés fondamentaux des citoyens tout en en encourageant l'innovation, en permettant l'émergence de nouveaux besoins et de nouveaux acteurs.

Faire autrement ne ferait que réduire d'autant la concurrence : par leur place essentielle, les fournisseurs d'accès à Internet sont en mesure de tordre en leur faveur la concurrence sur le marché des terminaux.

Nous attirons également l'attention du régulateur sur le fait qu'il est malsain que les fournisseurs d'accès à Internet aient une trop grande place sur ce marché : placer sous la domination de la même entreprise et l'accès au contenu, et le terminal, et dans certains cas le contenu amène à une domination de l'acteur en question sur l'utilisateur final qui n'est absolument pas désirable.

3.3 Question n° 10.

Demain, y aura-t-il encore un terminal focal pour le foyer ? Quel sera-t-il ?

L'expression « terminal focal pour le foyer » se comprend mal, et elle n'apparaît dans le rapport que pour cette question, qui manque cruellement de contexte. En l'absence d'autres précisions, nous postulons qu'elle désigne le terminal central dans le foyer, place qu'a occupé la télévision pendant de nombreuses années. Cette question est trop floue : il est difficile de savoir de quelle information a besoin le régulateur pour avancer ici.

Par ailleurs, cette question présuppose une pensée de l'économie de l'attention, donc de la consommation de contenus, avec le terme « focal » (focaliser de l'attention). Penser en ces termes empêche de penser Internet comme autre chose qu'un espace pour monétiser un acte de consommation de contenu, entièrement passif : c'est le rapprocher de la télévision, dont il est structurellement l'exact contraire, puisqu'il permet –et le règlement européen le rappelle– à chacun de *fournir* les contenus et services de son choix [15]. Le terminal ne *doit pas* être pensé uniquement comme un simple espace de consommation. Attention aux termes choisis pour aborder le problème, ici, ils posent le mauvais cadre de réflexion.

3.4 Question n° 11.

Les terminaux de demain seront-ils selon vous de simples lecteurs d'applications dans le cloud ?

Ce qui est important ici, c'est moins le pronostic plus ou moins fondé selon lequel les terminaux de demain deviendraient de simples lecteurs d'application que la question : est-ce que c'est souhaitable ?
En effet, toute prédiction de ce type sur les technologies de demain est toujours fondée sur des présupposés, qu'il convient d'interroger avant de prendre pour acquis ce qu'il en découle.

15. La maintenant classique conférence de Benjamin Bayart, intitulée « Internet ou Minitel 2.0 ? » le rappelle.

Ici, poser le terminal comme simple lecteur d'application pose des problèmes en partie liés à ceux évoqués dans notre réponse à la question 14. En posant le terminal comme un simple outil de consultation, on lui retire la fonction qu'il a, du moins avec les terminaux « fixes » d'être un outil de production et de diffusion de contenu. De plus, il rend l'utilisateur final dépendant, d'une part au réseau (sans connexion à Internet, une partie des fonctionnalités ne seront pas disponibles), d'autre part d'une machine qu'il ne contrôle pas, puisque les fonctions critiques sont reportées sur les applications hébergées par les soins d'un acteur économique –qui se réservera le droit d'en restreindre ou d'en interdire l'accès sur la base de critères arbitraires, sans recours possible. Ce futur n'est pas envisageable.

Une question subsidiaire non moins importante est : à quelles conditions ?
Il nous semble primordial que les changements, quels que soient leur nature, dans les terminaux, se fassent dans le respect des principes fondamentaux suivants :

— Décentralisation ;
— Logiciels libres ;
— Neutralité du Net ;

Si ce n'est pas le cas, alors le changement n'est pas souhaitable et tend vers une régression des droits de l'utilisateur final.

Enfin soulignons un dernier aspect de la question : le contrôle des données collectées, du consentement recueilli pour cette collecte et le stockage de ces données (lieu de stockage, durée de stockage, droit à la suppression des données stockées, ...).

3.5 Question n° 12.

5G – terminaux : lequel conditionne l'autre ?

Les deux vont ensemble et évoluent continuellement de manière étroitement liée. Les usages sont conditionnés par les moyens disponibles qu'ils soient applicatifs ou matériels. Les terminaux ainsi que les infrastructures sont créés en fonction de ces besoins et de la demande qu'ils créent. La 5G n'est qu'un moyen comme un autre. Rien ne justifie la remise en cause de la neutralité du Net, comme souhaitent le faire croire les fournisseurs d'accès à Internet historiques [16].

3.6 Question n° 13.

Le logiciel libre peut-il permettre d'améliorer les terminaux ?

Sans surprise, nous sommes convaincus que c'est le cas.

D'abord, pour des raisons techniques : la présence de logiciel libre sur les terminaux garantit, de manière générale, une meilleure sécurité. En effet, le code étant relu par la communauté, il sera très difficile d'y introduire, sans que cela se se sache, du code malveillant. Cette ouverture du code permet aussi, de manière générale, une bonne

16. `https://www.laquadrature.net/fr/Neutralit\%C3\%A9-du-Net-bilan-gris-fonc\%C3\%A9`

qualité technique des logiciels, pour les mêmes raisons d'évaluation du code par les pairs.

De plus, un logiciel libre ; parce qu'il est auditable par la communauté, est transparent : il est facile –pour un peu qu'on sache programmer ou qu'on puisse se faire expliquer le programme– de savoir quels traitements sont opérés sur les données personnelles des utilisateurs. Il est donc d'autant plus simple d'informer les utilisateurs sur ces traitements. Les logiciels propriétaires n'ont pas cette chance : il faut qu'une association (comme par exemple Exodus Privacy [17]) se monte pour aller regarder quels sont les trackers utilisés dans chaque application pour informer les utilisateurs. Le code étant opaque, il est impossible, sans aller vérifier par la pratique, de savoir comment les données de l'utilisateur sont traitées.

Le logiciel libre, parce qu'il est basé sur des standards ouverts, est *per se* interopérable : les difficultés soulevées à plusieurs reprises dans notre réponse à cette consultation dans d'autres réponses concernant la migration des données ou les changements d'OS sont fortement atténuées par l'utilisation du logiciel libre.

Enfin, ces caractéristiques ensemble allongent la durée de vie du logiciel : il est plus probable que la compatibilité entre les versions et avec les terminaux (même les plus anciens) soit conservée, que les fichiers restent lisibles plusieurs années après leur création, et que le support soit assuré sur un plus long terme que pour les logiciels propriétaires. C'est notamment cet argument qui avait poussé la Gendarmerie Nationale à passer au logiciel libre : est ce que le format .docx utilisé pour les documents Microsoft Word sera encore lisible dans cinq ans ? Rien ne le garantit. Pour ce qui est du format .odt, il est probable qu'il existe toujours des logiciels capables de lire ce format. La différence ici se fait aussi dans le partage des fins poursuivies par les uns et les autres : une entreprise privée ne cherche qu'à garantir des revenus à ses actionnaires. Si cela passe par faire racheter aux utilisateurs le dernier terminal parce que rien n'est plus compatible avec les anciennes versions de celui-ci, ou par cesser de maintenir un format de fichier, alors elle le fera. Une association loi 1901 ne nourrit aucun actionnaire : elle a intérêt à ce que les logiciels soient pérennes et les formats avec eux.

3.7 Question n° 14.

Le navigateur pourra-t-il remplacer l'OS ?

Il est possible de faire de plus en plus de choses au sein d'un navigateur, notamment d'accéder aux capteurs du terminal (capteur d'environnement, caméra, ...). Certaines fonctionnalités sont cependant limitées dans un navigateur comme l'accès direct au système de stockage du terminal. Il est donc probable que les navigateurs puissent tenir lieu d'OS. Il existe déjà des initiatives qui vont dans ce sens : Firefox OS, l'OS mobile développé par Mozilla, maintenant abandonné [18], et Chrome OS, le système d'exploitation basé sur le navigateur Chrome développé par Google [19].

17. `https://exodus-privacy.eu.org`
18. `https://fr.wikipedia.org/wiki/Firefox_OS`
19. `https://fr.wikipedia.org/wiki/Chrome_OS`

Le fait que l'usage des « progressive web apps » progresse pourrait permettre de centraliser davantage de tâches dans le navigateur. Comme toujours, le problème de la centralisation dans un système est le risque d'enfermement de l'utilisateur et la perte de contrôle sur ses données ainsi que sur l'utilisation de ce système (ici le navigateur). Le but est donc que quelle que soit l'évolution, l'utilisateur conserve le contrôle du terminal et du fonctionnement global y compris pour le navigateur. En particulier, la migration des données d'un navigateur vers un autre devra aussi inclure les données des applications qui s'y exécuteront. Ce n'est pas possible actuellement.

Rappelons encore que le règlement sur l'Internet ouvert prévoit que l'utilisateur doit pouvoir non seulement accéder aux informations et aux contenus, mais aussi les diffuser, ou fournir des applications et services, quel que soit l'équipement terminal (article 3). Il faudra donc être attentif à ce qu'une évolution vers les « progressive web apps » n'enferme pas ceux-ci dans une utilisation uniquement passive (consultation).

3.8 Question n° 15.

Réalité augmentée et réalité virtuelle : des terminaux inédits ?

La question intéressante ici est moins : est ce que la réalité augmentée ou virtuelle peut-être analysée comme un terminal inédit, mais : qu'est ce que ces technologies impliquent dans la manière dont nous nous servons des machines ?

D'ailleurs, l'immersion dans des mondes virtuels est quelque chose d'assez peu neuf : la plateforme *Second Life* a été lancée en 2003. Si les équipements pour le faire ont énormément évolué, les principes, eux, sont loin d'être inédits. Sur ces derniers, la lecture du passage concernant les mondes virtuels dans l'ouvrage d'Antonio Casili intitulé *Les liaisons numériques* peut être éclairante [20].

Il faut également rappeler qu'aujourd'hui, la quasi totalité des applications proposant des fonctionnalités de type reconnaissance de visage, reconnaissance de la parole etc. s'appuient sur des services tiers proposés par un nombre extrêmement restreint de gros acteurs (GAFAM). En effet, le développement des modèles nécessaires pour fournir ce type de fonctionnalités nécessite, en plus d'une forte expérience technique, l'accès à des sources massives de données pré-traitées (photos labellisées, enregistrements audio retranscrits etc.). Quelques gros acteurs seulement ont eu l'opportunité, en profitant de leur position dominante dans certains secteurs, de collecter ces corpus de données. Cela leur a permis de prendre une avance considérable sur les nouveaux acteurs qui souhaiteraient se positionner sur ce type de services. Et cette tendance continue à se renforcer par le fait que ces quelques acteurs sont devenus incontournables pour les développeurs d'applications, et continuent donc de bénéficier d'une position privilégiée pour la collecte de données et l'amélioration de leurs modèles. La conséquence étant l'émergence d'un écosystème à deux niveaux : une multitude de « petits » acteurs en concurrence, mais tous tributaires d'une poignée de gros acteurs, seuls capables de rivaliser les uns avec les autres.

20. Antonio Casilli, *Les liaisons numériques. Vers une nouvelle sociabilité ?*, Seuil, coll. « La couleur des idées », 2010

Pour l'utilisateur, cette situation aboutit donc à une illusion de choix entre une multitude d'applications n'étant que de simples façades derrière lesquelles on retrouve les quelques mêmes fournisseurs de service.

On peut se demander de quelle manière on peut permettre à de nouveaux acteurs de venir concurrencer les gros fournisseurs de services autour de l'Intelligence Artificielle. Une possibilité pourrait être la mise à disposition de corpus permettant l'entraînement de modèles performants, ou la mise en place d'obligations pour les acteurs utilisant les données des utilisateurs de devoir leur mettre à disposition les modèles créés à partir de leurs données (de façon similaire au principe de Licence Libre).

Enfin, rappelons que les données massivement stockées et traitées par ces technologies sont probablement des données personnelles. Le cadre dans lequel ces grands corpus de données ont été rassemblés pose donc quelques questions : en premier lieu, est-ce que les utilisateurs ont pu choisir, de manière libre et éclairée, de consentir au traitement de leurs données ? quelles garanties de sécurité, concernant des données aussi sensibles que celles qui permettent la reconnaissance faciale, par exemple, sont apportées à l'utilisateur final ? Qu'est-ce que cela veut dire, qu'une société privée possède un *fichier* d'éléments extrêmement sensibles tels que l'image de la rétine, de ses clients ? La centralisation au sein d'un très petit nombre d'entreprises de ces fichiers sensibles sur des millions de personnes dans le monde ne pose-t-elle pas problème ?

3.9 Question n^o 16.

Le véhicule connecté est-il un terminal comme les autres ?

Cette question est large et appelle à une réponse complexe, et forcément nuancée.

Sur le plan strict du réseau, le véhicule connecté vient répondre, comme d'autres terminaux, aux besoins de l'utilisateur, en utilisant les mêmes protocoles pour communiquer sur Internet. Pour l'antenne qui lui délivre le trafic, il n'y a effectivement aucune différence entre une voiture et une tablette : c'est un terminal comme un autre. Il n'y a pas de raison technique valable de prioriser le trafic de la voiture sur celui de la tablette.

Ceci dit il reste que faire communiquer un véhicule critique –et rendre son fonctionnement dépendant, pour tout ou partie, du réseau– est une mauvaise idée : rappelons d'ores et déjà que ces véhicules, contrairement à ce que les opérateurs tant attachés à la 5G avancent, ne doivent surtout pas devenir dépendants du réseau, fût il aussi performant qu'on nous le promet ici –aucun réseau n'est infaillible. Nous revenons là-dessus un peu plus bas.

Sur le plan de la société, on aurait tort de se comporter exactement comme cette antenne 4G en mettant sur le même plan ces deux objets. Si ces derniers utilisent Internet pour rendre service à l'utilisateur final, est-ce à dire qu'ils doivent être considérés tout à fait de la même façon ? La voiture lancée sur l'autoroute met en jeu des vies humaines, qui font confiance au programme qui « conduit » la voiture pour arriver à destination (dans le cas d'une voiture non pas seulement connectée mais autonome). Il n'y a pas un risque vital de ce type avec l'utilisation d'une tablette. Pour pasticher Dostoïevsky,

on ne peut pas comparer Shakespeare et une paire de bottes uniquement parce que les deux communiquent par Internet.

Paradoxalement, ces deux aspects sont compatibles à notre sens : le fait que la voiture soit un terminal particulier parce qu'il engage de manière critique la responsabilité de ceux qui la construisent et la conduisent ne remet pas en cause le respect de la neutralité du réseau. Un véhicule connecté ne devrait pas avoir besoin, par exemple, d'une voie privilégiée sur Internet pour fonctionner. Pour des raisons de sécurité, il doit pouvoir se passer de réseau, afin que les pannes éventuelles ne gênent pas son fonctionnement. Rester dans le respect d'un Internet neutre n'empêche absolument pas une utilisation *exceptionnelle* du réseau, par exemple pour signaler d'urgence la localisation du véhicule lors d'un accident.

Pour finir, le fait que la voiture engage un risque vital rend primordiales d'une part la sécurité (il faut que la voiture ne soit pas exposée à des fuites de données ou qu'on puisse en prendre le contrôle de manière malveillante comme cela a déjà été démontré sur les Jeep Cherokee en 2015, par exemple), et d'autre part la confiance. Sur ces questions, il semble que le maitre mot soit le contrôle de l'utilisateur final. Le fait que la voiture soit connectée ne doit pas le déposséder du contrôle qu'il peut avoir de la machine qu'il a en sa possession, ni de son libre-arbitre. Ceci vaut aussi pour d'autres terminaux : il doivent *toujours* être sous le contrôle de l'utilisateur.

On peut aussi renverser complètement cette question et considérer que la voiture n'est *pas* un terminal : ses fonctions de communication sont en tout point *accessoires* à sa fonction première qui est de permettre le transport de personnes et de biens. En ce sens, elle ne doit *pas* être analysée comme un terminal de télécommunications. Encore une fois, cela n'empêche en rien que ses fonctions de communications respectent la neutralité du Net.

Au final, il y a deux alternatives : ou l'on considère que la voiture connectée est un terminal, mais alors il doit être pensé de manière particulière, pour concilier son aspect critique et son statut d'objet communiquant sur Internet, ce qui est extrêmement compliqué, d'autant plus dans les conjonctures de pression actuelle de la part des acteurs du marché, ou l'on ne considère pas la voiture comme un terminal du tout. Dans tous les cas, il semble qu'il manque les bonnes catégories pour penser ce type d'objet sans se tromper dans l'analyse.

3.10 Question n° 17.

Où et comment placer le curseur entre sécurité du terminal et ouverture aux tiers ?

Il semble que la question s'intéresse à l'accès aux terminaux par des tiers au titre des multiples applications installées dessus.

On peut acter qu'à l'ère où la donnée personnelle est le nouvel or noir des entreprises et où celle-ci se concentre dans le terminal mobile, qui accompagne maintenant partout bon nombre d'utilisateurs finals, il est important d'avoir des terminaux dont la conception prend en compte la protection de la vie privée, « by design ».

L'utilisateur doit pouvoir avoir confiance dans son terminal et dans le fait qu'il ne sera pas la source d'une fuite de données. L'utilisateur doit être informé de l'utilisation des permissions demandées, avec une application stricte des principes du règlement général pour la protection des données (RGPD) sur l'information et le consentement. Le terminal doit pouvoir être mis à jour facilement et régulièrement, le fabricant doit fournir les mises à jour de sécurité sur l'ensemble de la durée de vie du produit, les mises à jour de sécurité doivent pouvoir être installées sans devoir accepter des changements de conditions d'utilisation. Le terminal doit être sécurisé contre les intrusions en provenance du réseau.

Si le terminal n'est pas sous le contrôle de l'utilisateur, les garanties en matière de sécurité et de protection de la vie privée sont bien faibles.

4 Thème n° 3 : Quels sont les freins au changement de terminal ou d'OS ?

4.1 Question n° 18.

Quelles sont les difficultés rencontrées lors d'un changement d'OS ? La problématique est-elle identique sur le mobile et sur le fixe ?

Nous répondons aux questions 18 et 19 en même temps ci-dessous.

4.2 Question n° 19.

Les outils disponibles pour faciliter le passage d'un système d'exploitation à un autre sont-ils performants ?

Les difficultés de changement d'appareil et de système d'exploitation sont :
— la migration des données (y compris des films et vidéos soumis aux DRM),
— la migration des configurations,
— la migration des applications ou l'installation d'alternatives,
— la compatibilité des autres équipements.
Plusieurs cas sont à distinguer : la migration d'Android vers iOS, la migration d'iOS vers Android, sur des terminaux mobiles, et finalement tous les autres cas.

Migrer d'Android vers iOS peut se faire en utilisant l'application « Move to iOS » développée par Apple et publiée sur le Play Store de Google. Les données seront échangées en WiFi directement entre les appareils.

Migrer d'iOS vers Android peut être effectué au travers de l'application « Google Drive » développée par Google et publiée sur l'App Store d'Apple. Les données seront d'abord exportées vers les serveurs « cloud » de Google avant de pouvoir être utilisées depuis un appareil Android.

Dans les deux cas cités ci-dessus, la copie des données et des configurations est le plus souvent maîtrisée par l'éditeur du système d'exploitation. Ce dernier facilite ainsi la migration entre appareils utilisant le même système d'exploitation mais la complexifie dans les autres cas. Il est donc nécessaire d'avoir des comptes auprès d'Apple et de Google, voire de faire stocker ses données sur les serveurs de l'un, afin de disposer d'une méthode de migration pratique mais pas nécessairement rapide. Cela pose des questions évidentes en matière de consentement et de protection des données : que vaut le consentement d'un utilisateur qui accepte les conditions générales de Google Store *uniquement* parce qu'il y est contraint pour transférer ses données d'un terminal à un autre ? En d'autres termes, dans ce contexte, il faut, si l'on veut changer de système d'exploitation, entrer dans une relation contractuelle (relativement biaisée) avec les *deux* éditeurs majeurs du marché.

Nous n'évoquons ici que le transfert des données personnelles de l'utilisateur : il faut également prendre en compte le fait que toute application –pour autant qu'elle soit disponible sur les deux magasins d'applications principaux– achetée d'un côté devra être rachetée de l'autre.

Enfin, il est important de noter que ces outils de migration ou de synchronisation de données sont focalisés sur le transfert entre les écosystèmes des deux plus gros éditeurs du secteur des terminaux mobiles (tablettes, *smartphones* de Google et Apple) : ils ne sont pas applicables à d'autres cas. Pour ceux-ci, il n'existe pas d'outil fiable de migration. Si l'interopérabilité entre Windows et MacOS, par exemple, s'améliore, il faut déplorer que, en ce qui concerne les ordinateurs (fixes ou portables), l'interopérabilité très faible des systèmes (formats de fichiers propriétaires, notamment), ajoutée à l'absence d'outil fiable rende particulièrement malaisé le passage de Windows à MacOS, ou l'inverse, ou le passage à une distribution Linux –opération qui s'est grandement simplifiée avec l'arrivée de la distribution Ubuntu.

Notons que sur les terminaux fixes, l'utilisateur a généralement la possibilité d'accéder directement à toutes ses données et il lui est donc possible d'effectuer des sauvegardes et des copies entre les systèmes. L'opération est peut-être relativement longue mais a encore aujourd'hui le mérite d'être faisable. Mais la tendance de Microsoft et d'Apple pour les terminaux fixes est de reproduire le fonctionnement du mobile, plus fermé et moins maîtrisé par l'utilisateur, au lieu de faire l'inverse - ce qui serait souhaitable.

4.3 Question n° 20.

Quelles sont les difficultés rencontrées par des acteurs qui voudraient élaborer des outils de migration alternatifs ?

De manière générale, on constate, comme on l'a dit plus haut, qu'il n'y a pas d'application tierce en mesure de réaliser une sauvegarde intégrale d'un système de manière simple (au minimum, dans le cas d'un terminal mobile, il est nécessaire de « rooter » le téléphone ou d'activer des options développeur par exemple). La raison avancée est la sécurité du système contre les applications malveillantes mais une permission explicite correspondante semble ensivageable. Offrir aux développeurs d'applications des moyens

techniques de réaliser des applications de sauvegarde et de restauration avec une interaction utilisateur acceptable est un prérequis à l'apparition de telles applications.

On peut également envisager d'encourager, par exemple pour la migration des données personnelles de l'utilisateur, l'utilisation de formats ouverts, interopérables *per se* : cela simpliferait une partie des opérations de migrations qui consistent en la conversion de fichiers d'un format propriétaire à l'autre, ou encore la standardisation entre les différents OS, « fixes » (Windows, MacOS, GNU/Linux) ou mobiles (iOS, Android, etc.) de certains éléments (comme par exemple où se situent les fichiers de configuration) pour rendre plus transparentes les opérations de migration. Il est relativement trivial de passer d'une distribution Linux à une autre parce que le système étant ouvert, il est de fait standardisé : un certain nombre de paramètres choisis par l'utilisateur sont ainsi conservés. A défaut de *tout* ouvrir, il semble souhaitable que les acteurs du secteur se mettent d'accord sur un standard minimal, dans l'intérêt de l'utilisateur final.

4.4 Question n° 21.

Certaines limites au changement de plateforme ne résultent-elles pas des formats propriétaires et DRM ?

En effet : nous avons déjà évoqué le frein que consistait l'usage de formats de fichiers propriétaires, et les DRM allant plus loin, ils sont d'autant plus à voir comme des freins majeurs.

Les DRM participent à l'enfermement et à la surveillance des utilisateurs dans un système (cf. les DRM dans les *ebooks*, par exemple, qui sont également placés là pour surveiller ce que lit l'utilisateur final). Ils vont à l'encontre de l'ouverture des terminaux et d'Internet, de la maîtrise des utilisateurs de leurs terminaux et des contenus. C'est un choix fait par les industriels contre la volonté des utilisateurs finals, car les industriels ont le pouvoir de faire ce choix d'enfermer des utilisateurs.

L'enfermement des utilisateurs est infantilisant puisqu'ils deviennent totalement dépendants des industriels et fournisseurs de services qui utilisent des formats propriétaires et DRMs.

4.5 Question n° 22.

La portabilité des données via le cloud présente-elle un intérêt particulier ? Comment l'organiser efficacement ?

La portabilité des données via le *cloud* présente un intérêt au même titre que la portabilité des données via d'autres médias ; malheureusement, même lorsque d'autres méthodes sont techniquement disponibles, l'utilisation du *cloud* (propriété de l'éditeur du système d'exploitation) est celle qui est tout particulièrement mise en avant. Nous ne voyons pas de raison technique pour une telle différence de traitement. La raison semble donc être de continuer à enfermer l'utilisateur dans un système qu'il ne contrôle pas, et

le déposséder ainsi de ses données, ses habitudes, sa volonté et d'en profiter, au passage pour collecter ces données pour des usages que les plateformes de *cloud* sont libres de se réserver dans les conditions d'utilisation du service. Dans ces conditions, ça ne présente pas d'intérêt pour l'utilisateur final, c'est plutôt le contraire qui se produit dans les faits.

4.6 Question n° 23.

Une percée du modèle de l'abonnement mensuel aux applications permettrait-elle de réduire la difficulté à changer d'OS ? Cela ne signifie-t-il pas que les utilisateurs se lient à leur fournisseur de contenus plutôt qu'à leur terminal ?

Nous ne pensons pas que cela résolve quoi que ce soit. Comme envisagé dans la question, la différence principale serait que l'utilisateur verrait ses données enfermées non pas chez l'éditeur du système d'exploitation mais chez l'éditeur du logiciel. Il semble impensable de considérer cela comme une amélioration.

La question, telle que formulée par l'ARCEP, est intéressante car à aucun moment la proposition de systèmes plus ouverts est émise. C'est pourtant la seule solution aujourd'hui qui permettrait aux utilisateurs de reprendre le contrôle de leurs terminaux, de changer d'OS quand bon leur semble, mais aussi qui permettrait une meilleure concurrence entre les différents systèmes puisqu'ainsi iOS et Android ne seraient plus les deux systèmes tout-puissants sur le marché, mais deux systèmes parmi de multiples OS libres.

4.7 Question n° 24.

Les incompatibilités physiques entre les appareils de différents univers sont-elles encore déterminantes ?

La motivation derrière ces incompatibilités physiques n'est qu'un argument de plus pour garder l'utilisateur enfermé. Or les arguments en faveur d'un type de connecteur ou d'un autre, par exemple, sont devenus obsolètes avec les connecteurs USB de type C. Le fait pour les industriels de refuser la compatibilité entre les appareils est un moyen de réduire la concurrence qui peut être efficace. On imagine en effet mal un « dock » avec enceinte qui aurait plusieurs connecteurs ou des adaptateurs pour chaque type d'appareil. Ces incompatibilités ont donc toujours des conséquences négatives.

5 Pistes d'action considérées

5.1 Question n° 25.

Est-il souhaitable d'améliorer l'information des utilisateurs et des pouvoirs publics concernant les positions et les pratiques des fabricants de terminaux et de systèmes d'exploitation ?

La réponse est dans la question. Il est totalement anormal que les fabricants de terminaux et d'OS puissent mettre en place des pratiques anti-concurrentielles avec des conséquences très fortes sur l'infantilisation des utilisateurs, en toute impunité. L'information est un préalable, mais ce ne sera pas suffisant pour faire changer des pratiques qui devraient être aujourd'hui considérées comme illégales au regard du droit de la concurrence et du droit concernant la protection des données.

5.2 Question n° 26.

Les outils envisagés paraissent-ils pertinents ?

La proposition a) pourrait être une première étape, mais n'est pas suffisante en tant que telle. La transparence n'empêche pas les pratiques discriminantes, notamment lorsque – discrimination ou pas – les utilisateurs sont enfermés dans un environnement et qu'ils n'ont pour seule porte de sortie qu'un autre environnement tout aussi enfermant et infantilisant. C'est le cas sur les OS mobiles car les alternatives libres sont utilisables uniquement par des personnes ayant un bon niveau technique.

La proposition b) regroupe en fait plusieurs éléments. Comme nous ne savons pas s'ils sont cumulatifs, nous les détaillons ici :

– *les fabricants de terminaux pourraient être incités à supporter des solutions susceptibles d'être compatibles avec tous les équipements, comme les progressive web apps ;*
Les incitations risquent d'être peu efficaces et il faudrait rapidement mettre en place des obligations pour imposer la compatibilité des terminaux avec ces solutions. Voir aussi notre réponse à la question n° 3.

– *tout en veillant à ne pas brider l'innovation, il pourrait être utile de promouvoir une meilleure compatibilité matérielle entre les équipements des différents univers ;*
Il semblerait qu'une obligation de compatibilité matérielle encouragerait l'innovation en favorisant des rapports plus concurrentiels. Voir aussi notre réponse à la question n° 24.

– *pour certains fabricants de terminaux et développeurs d'OS disposant d'un fort pouvoir de marché, il serait concevable de proscrire l'offre exclusive de certains contenus.*
Pour tous les fabricants de terminaux et développeurs d'OS, la réglementation européenne sur l'Internet ouvert proscrit l'offre exclusive de certains contenus. Le règlement précise bien que « Les utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'Internet. » (art.3 du Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un Internet ouvert [21]). D'autre part, le considérant 7 du même règlement est très clair sur la nécessité d'interdire les accords ou pratiques commerciales qui réduisent le choix des

21. http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX\%3A32015R2120

utilisateurs finals, notamment lorsque les FAI ou fournisseurs de contenus, d'applications et de services concernés disposent d'un fort pouvoir de marché.

– *les magasins d'applications alternatifs pourraient être encouragés, notamment en levant les freins à l'installation de tels magasins par les utilisateurs ;*
Oui. Ce serait très désirable en effet.
Ce serait notamment possible via l'installation de magasins comme F-Droid via Google Play Store ou App Store. Voir notamment notre réponse à la question n° 7.

– emphles développeurs de systèmes d'exploitation pourraient se voir imposer l'ouverture de leurs API, afin de mettre sur un pied d'égalité l'ensemble des développeurs.
Bien que ce soit théoriquement déjà le cas sur Android, certaines permissions sont uniquement accessibles par ajout sur liste blanche (contenant par défaut uniquement des applications développées par Google) dont la modification nécessite des manipulations techniques inaccessibles à un utilisateur même « avancé ». Sur iOS, ce n'est même pas théoriquement possible. Les éditeurs de système d'exploitation ont donc un avantage net qui porte atteinte à la concurrence et réduit drastiquement les possibilités d'innovation.

5.3 Question n° 27.

Les utilisateurs bénéficient-ils d'un choix suffisant en termes de terminaux et de système d'exploitation ?

Nous répondrons à cette question en distinguant les différents terminaux et les systèmes d'exploitation. La situation n'est pas tout à fait la même selon les terminaux.

En ce qui concerne les téléphones mobiles, la réponse est mitigée : au niveau matériel, si le choix est relativement vaste du côté des terminaux Android, on constate que, du côté des terminaux Apple, le terminal et son OS sont couplés : on ne peut choisir l'un sans l'autre. Au niveau des OS, si la majorité des terminaux se partage maintenant entre Android et iOS, ce qui est loin de constituer un éventail de choix suffisant, il convient de noter l'existence d'OS mobiles alternatifs, comme LineageOS ou Replicant (il en existe d'autres). Nous renvoyons notamment à notre réponse à la question n° 6 qui évoque une partie des freins à leur développement.

En ce qui concerne les PC (fixes ou portables), le choix des terminaux est plutôt convenable, bien que la grande concentration des constructeurs de matériel informatique soit inquiétante : ces constructeurs sont à même de poser leurs conditions, d'imposer des standards de fait, ou encore de faciliter l'installation de portes dérobées dans leurs matériels. Cela rend aussi vulnérable le terminal de l'utilisateur final : c'est ce que montrent les récentes affaires de failles de sécurité dans les processeurs AMD, ARM et Intel (*Spectre* et *Meltdown*[22]). La quasi totalité des processeurs utilisés aujourd'hui sont vulnérables, puisqu'ils proviennent en grande majorité des constructeurs principaux, concernés par la faille.

22. http://www.liberation.fr/planete/2018/01/05/intel-les-ordinateurs-touches-en-plein-core_1620659

Nous rappelons également au régulateur le fait que la plupart des PC vendus sont pré-installé avec l'OS Windows, ce qui signifie que même si l'utilisateur final ne veut pas utiliser cet OS et en installe un autre, il aura payé la licence Windows en même temps que sa machine. C'est un phénomène de vente liée classique [23]. Nous ne développons pas, cette question est largement abordée par l'April [24]. Il faut noter également que l'opération qui consiste à installer un autre OS sur sa machine, si elle est de plus en plus accessible au grand public, reste parfois compliquée pour les OS majoritaires (voir notre réponse à la question 20). Par exemple, il faut maintenant passer par un certain nombre de paramétrages savants sous Windows 10 pour permettre à la machine de démarrer sur une autre système d'exploitation, chargé sur un support amovible, préalable à toute installation d'OS.

Ainsi, le choix entre les deux systèmes d'exploitation majoritaires (Windows et MacOS) est non seulement totalement insuffisant (manque de concurrence, d'innovation, de liberté de choix) mais la restriction de choix est renforcée par la vente liée.

Par ailleurs, si nous continuons à analyser la « box » comme un terminal, cette question devient vraiment intéressante. En effet, on observe que le choix en question est de fait quasiment inexistant : dans la plupart des cas, l'utilisateur final se voit imposer un routeur, qui est celui qu'il loue à son fournisseur d'accès à Internet. Cette absence de choix n'est pas liée à des contraintes techniques : l'utilisateur final pourrait très bien avoir son propre routeur et l'avoir configuré pour qu'il lui permette de se connecter à Internet –pour un peu que le FAI documente la configuration nécessaire à la connexion à son réseau. Pour disposer du *triple play*, il dispose souvent d'un décodeur TV prévu à cet effet et séparé de la « box » qui assure la fonction de routeur domestique. En outre, pour disposer d'une connexion FTTH, il n'est pas rare que l'équipement en charge du traitement du signal optique (l'ONT) soit aussi découplé de la box. Cela nous permet de considérer que la box est un terminal [25]. La « box » du FAI pourrait très bien être remplacée par un autre matériel équivalent.

Il se trouve en réalité que la « box » permet de fournir un certain nombre de services supplémentaires à l'utilisateur final, comme jouer à des jeux vidéo. Cette mise à disposition de services non liés à la fourniture d'accès à Internet *via* la « box », en l'absence d'un marché grand public permettant de choisir son terminal en fonction de ses besoins, est un levier supplémentaire pour rendre le client d'autant plus captif. Si l'utilisateur final n'en a pas besoin, il n'a pas d'autre choix que s'en accommoder. S'il est suffisamment expert en informatique, il pourra certainement remplacer sa box par un routeur dont il assurera la configuration adéquate au prix de quelques recherches (puisque cette opération n'est pas documentée par les opérateurs, l'utilisateur final étant supposé utiliser la « box »). On notera que même s'il ne l'utilise pas, rien n'est prévu dans le contrat avec l'opérateur pour que l'utilisateur puisse rendre sa « box » : il continuera à en payer la location tous les mois, même si cette dernière dort sagement dans un carton.

23. Bien que, à notre grande surprise, la Cour de justice de l'Union européenne soit d'un autre avis `https://www.nextinpact.com/news/101268-la-justice-europeenne-sanctuarise-vente-liee-pc-et-os.htm`

24. `https://www.april.org/groupes/vente-liee`

25. Voir l'article de Benjamin Bayart sur la liberté de choix du terminal `http://blog.fdn.fr/?post/2016/05/18/Liberte-de-choix-du-terminal`

A quoi peut-on le mesurer ?

Il y a un nombre plutôt élevé de terminaux mobiles disponibles et deux systèmes d'exploitation majoritaires. Il n'y a probablement pas besoin de mesure spécifique pour remarquer que le choix entre les systèmes d'exploitation est extrêmement limité.

5.4 Question n° 28.

Les outils envisagés semblent-ils adaptés ?

Cf. notre réponse à la question n° 26.