

Les terminaux sont-ils le maillon faible de l'ouverture d'internet ?

Les terminaux font aujourd'hui partie de la vie quotidienne de millions d'utilisateurs, au travers d'appareils de différents formats et en particulier d'appareils mobiles de type smartphone, tablette ou d'ordinateurs portables. Ces appareils ont permis de numériser bon nombre d'aspects de la vie, qu'il s'agisse des communications entre les individus ou la capture, le stockage et l'échange d'informations. Ces appareils disposent en effet de nombreuses entrées/sorties permettant de capter et d'interagir avec l'environnement, en récoltant et en stockant une très grande quantité de données tout au long de chaque journée. Ces données sont très largement stockées au sein d'infrastructures de stockage de différentes entreprises, le plus souvent des multinationales Américaines.

Ces appareils se caractérisent donc par une grande capacité à interagir avec les différents aspects du quotidien et une connectivité accrue permettant la communication et le partage de données, mais également par l'accès à de nombreux contenus et services en ligne. En effet, ces terminaux sont les passerelles d'accès pour l'accès rapide au web et à différents types de services, qui génèrent un grand nombre de méta-données et forment en cela une empreinte numérique de l'utilisateur, qui permettra son identification fine. Ces procédés d'identification sont par ailleurs connus pour être mis en œuvre par de nombreuses agences de renseignement.

Les utilisateurs peuvent donc légitimement se poser la question de la confiance qu'ils peuvent accorder à ces terminaux, en particulier du point de vue de leur fonctionnement et agissements réels vis-à-vis des données qu'ils traitent, mais également de leur sécurité, afin de s'assurer que ces données ne sont pas vulnérables et restent effectivement privées. Le contrôle de ces appareils apparaît ainsi comme un élément clef, en ce qu'il permet à l'utilisateur de s'assurer du bon fonctionnement de l'appareil tout au long de son utilisation. Il s'agit pour cela dans un premier temps d'être en mesure d'effectuer des audits du code utilisé sur l'appareil et de pouvoir le modifier et l'exécuter par la suite. Il devient alors possible pour l'utilisateur d'y apporter ses modifications personnelles ou celles de la communauté, de supprimer toute restriction volontaire de fonctionnalité mais aussi d'effectuer des audits de sécurité pour identifier les vulnérabilités et les portes dérobées et d'apporter des corrections indépendamment des constructeurs des appareils qui prennent rarement en charge les appareils de nombreuses années. Il s'agit également par là de garantir l'accès à la connaissance du fonctionnement des appareils, présentant ainsi une opportunité pour étudiants, curieux et passionnés d'étudier et de modifier des logiciels largement utilisés. De plus, la préservation de cette connaissance reste un enjeu pour assurer un certain contrôle à long terme de la technologie, toujours plus présente, de la part de la société toute entière.

Le règlement Européen 2015/2120 prévoit pour les utilisateurs « 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, ». La question du libre choix du terminal ouvre la porte à la possibilité pour l'utilisateur de pouvoir choisir des terminaux en lesquels ils peuvent avoir confiance, sur lesquels ils ont le contrôle et dont le fonctionnement est connu et largement diffusé. Le projet Replicant s'inscrit tout particulièrement dans cette démarche, en développant un système d'exploitation entièrement composé de logiciels libres, basé sur le code libre d'Android, diffusé par Google. Il s'agit, à partir de cette base libre, de développer les logiciels nécessaires à la prise en charge matérielle de différents appareils mobiles, de manière plus ou moins complète mais avec un minimum de fonctionnalités disponible. Replicant s'inscrit donc au niveau du système d'exploitation, mais les problématiques de la confiance, du contrôle et de la connaissance des appareils concernent plus largement l'ensemble des composants des appareils mobiles. S'il est en général aujourd'hui possible de remplacer le système d'exploitation de ces appareils, la tâche est autrement moins aisée pour d'autres composants critiques tels que les logiciels de démarrage, qui s'exécutent avant le système d'exploitation, mais également les environnements d'exécution de confiance qui

s'exécutent pendant toute la durée d'utilisation des appareils avec les privilèges les plus élevés sur l'appareil. Les appareils qui, en plus de présenter une connectivité TCP/IP à l'Internet sont également connectés au réseau GSM disposent d'un composant dédié à cette communication mobile, le baseband ou modem.

Tout comme les logiciels cités précédemment, le logiciel qui s'exécute sur ce modem est bien souvent protégé par une signature numérique qui rend impossible sa modification par quiconque ne possède pas la clef privée du fabricant, qu'il ne divulgue pas. Il est ainsi impossible d'exécuter du logiciel libre dans ces cas de figure, n'offrant ainsi jamais à l'utilisateur une véritable confiance, ni de véritable contrôle ou une connaissance complète de son fonctionnement.

De cette façon, on retire du pouvoir aux utilisateurs finaux, qu'il s'agisse d'individus ou d'entreprises intermédiaires qui utilisent et intègrent ces appareils, qui est alors dans les mains du fabricant des appareils. Il s'agit ainsi de consacrer l'union entre le matériel d'une part et le logiciel qui s'exécute sur celui-ci d'autre part. Pour autant, le logiciel se caractérisant comme des instructions pouvant être modifiées, il est une utilisation tout à fait légitime pour l'utilisateur de pouvoir modifier le logiciel s'exécutant sur chacun de ses appareils, qui est par nature dissocié de l'aspect matériel qui permet son exécution. On souhaite donc particulièrement insister sur cette distinction fondamentale, de l'appareil d'une part et du logiciel qu'il exécute d'autre part.

Cette capacité de modifier les logiciels présente par sa nature de nombreuses opportunités d'innovation par la très grande flexibilité qu'elle offre, qui permet l'élaboration d'applications et de services innovants qui sont tout à fait de nature à favoriser l'ouverture d'Internet et le développement de l'activité qui lui est associée.