

Focus actu



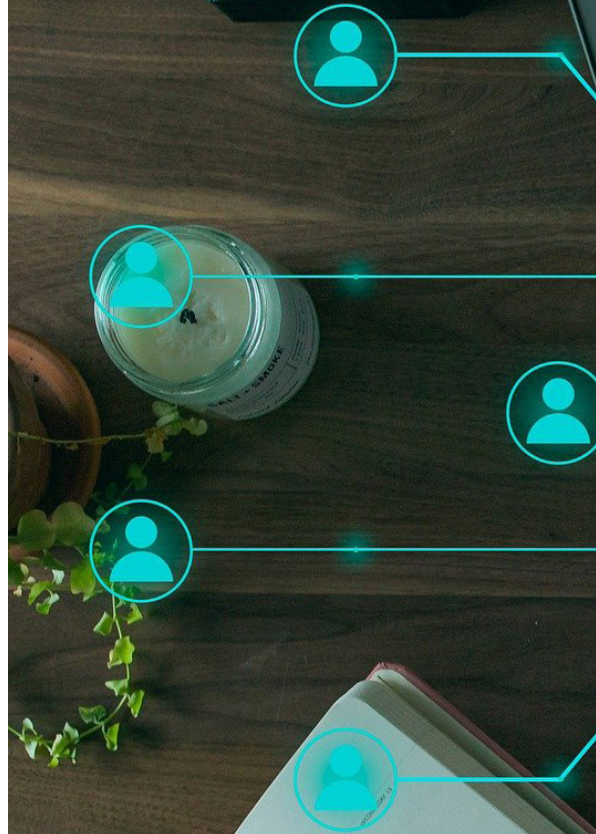
Rien à se reprocher, rien à cacher ? Vos smartphones au service de la protection de l'enfance

Disons que ce n'est pas seulement un sujet d'actu, mais aussi une question intemporelle : à quel point sommes-nous prêts à rogner notre droit à la vie privée pour assurer la sécurité de tous ? Vous sentez déjà venir le mal de tête ? Certains, pourtant, sont déjà en train de répondre à votre place.

Des bonnes intentions...

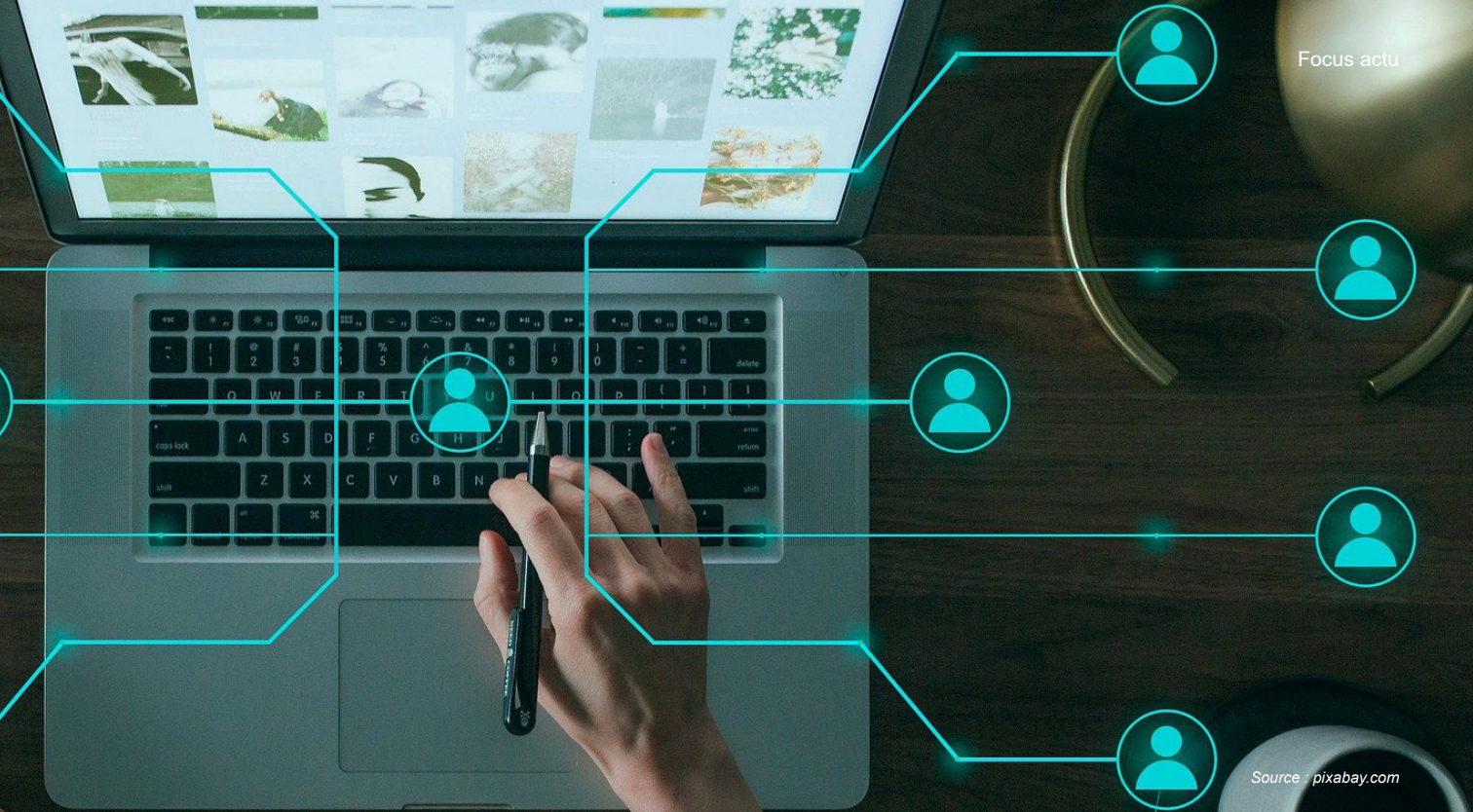
Cet été, une célèbre marque de smartphones a surpris nombre de ces *aficionados* en annonçant de nouvelles fonctionnalités liées à la protection de l'enfance. L'une d'entre elles déchaîna vite les passions : la possibilité de détecter automatiquement les potentielles photos à caractère pédopornographique se trouvant dans la bibliothèque du téléphone d'un individu, pour le signaler aux autorités compétentes. Cette détection implique que l'appareil compare systématiquement chaque image ajoutée par l'utilisateur avec une base de données d'empreintes numériques, déjà préchargée dans le système d'exploitation, renvoyant à du contenu illégal. Bien entendu, personne n'irait remettre en cause l'objectif poursuivi. La surprise

tient plutôt du moyen utilisé, alors même qu'Apple a fait de sa capacité à protéger la vie privée de ses utilisateurs un véritable argument marketing. Ainsi, à coups d'affiches publicitaires géantes défigurant les bâtiments les plus imposants de nombreuses capitales, la marque martèle depuis quelques années que « ce qui se passe sur ses téléphones reste sur ses téléphones ». Les autres géants du web, dont le *business model* se base à peu près uniquement sur l'accumulation et la monétisation de données privées, y sont tacitement dénigrés, dans une démarche très manichéenne. Facebook, dont le créateur affirmait dix ans plus tôt que la vie privée était « une norme sociale dépassée », voyait rouge, tant le message était vendeur.



Source : pixabay.com

Relief-F asbl



Des précédents inquiétants

Alors, changement de paradigme ? Peut-être pas. Faire des compromis avec un idéal de protection de la vie privée dans le but de mettre hors d'état de nuire des pédophiles semble être un tantinet plus justifiable et moins mercantile que de proposer quatre publicités ciblées pour deux photos de vacances dans un fil d'actu. Et pourtant, ça ne passe pas. Levée de boucliers de la part de chercheurs en sécurité, de militants des droits de l'Homme, de représentants de la Jeunesse et même de certains gouvernements.

C'est que le bilan d'Apple, quand il s'agit de se plier aux demandes d'états autoritaires pour préserver ses parts de marché, n'est guère rassurant pour l'avenir. Aujourd'hui, l'entreprise ne se prive pas de censurer toutes les applications mobiles qui dérangent les dictatures où il fait bon d'investir. Les détracteurs de la nouvelle fonctionnalité estiment qu'il n'est pas farfelu d'imaginer que demain, cette petite prouesse technologique soit utilisée par des gouvernements pour détecter systématiquement d'autres contenus que des images pédopornographiques, y compris au détriment de jeunes. Et ce, même à l'insu de la marque : encore cet été, une faille de sécurité présente sur une majorité des téléphones qu'elle proposait à la vente a permis l'espionnage, par des gouvernements, de 180 journalistes, 600 hommes et femmes politiques, 85 militants des droits humains ou encore 65 chefs d'entreprise du monde entier¹.

¹ https://www.rtbf.be/info/monde/detail_affaire-pegasus-des-experts-de-l-onu-demandent-un-moratoire-sur-la-vente-de-logiciels-espions?id=10822611

La problématique de la porte dérobée

Expliquons tout de même que tout un tas de garde-fous accompagnent ce mouchard bienveillant. Ainsi, il est nécessaire qu'il y ait de multiples occurrences dans la bibliothèque d'un smartphone pour que les employés de la marque examinent le cas, ce qui rendrait les « faux positifs » statistiquement négligeables. Dans les tests effectués, leur nombre s'élevait à trois pour 100 millions d'images scannées.



Reprécisons aussi que ce sont les métadonnées des images qui sont comparées et non les images elles-mêmes, que ce soit par la machine ou par l'humain en bout de chaîne qui décidera ou non d'avertir les autorités pour qu'elles enquêtent davantage. Encore heureux, et on ne doutait pas qu'il soit technologiquement possible qu'un employé lambda puisse exercer ce contrôle sans voir vos photos, mais là n'est pas la principale

préoccupation des associations de défense de droits de l'Homme. Ce qui les préoccupe, c'est la mise en place d'une *backdoor*, d'une porte dérobée sur vos données personnelles qui, si elle est détournée de sa finalité par des personnes mal intentionnées, permet la détection systématique d'autres types de contenus sans intervention humaine (si ce n'est lors de la mise en place du code malicieux).

Des fonctionnalités à double tranchant

L'annonce simultanée d'une seconde fonctionnalité permettant aux parents d'être prévenus, entre deux notifications, lorsque leur enfant consultait des images sexuellement explicites (y compris celles représentant des adultes consentants) n'a sans doute pas apaisé les esprits. Le contrôle parental existe depuis longtemps, certes. En revanche, le peu de prévoyance quant aux répercussions de telles dénonciations sur des jeunes LGBTQI et/ou vivant dans des foyers violents laisse perplexe nombre d'observateurs. Et les mêmes

questions se posent quant au détournement de la technologie de reconnaissance de contenus qui sera utilisée.

Face à toutes ces réactions, l'implémentation de ces fonctionnalités est retardée. Le temps de les rendre plus respectueuses de la vie privée, ou alors de mieux faire passer la pilule ? La marque à la pomme aurait-elle surestimé le prix à payer pour protéger nos bambins ? Pas sûr qu'on puisse l'obliger à revoir sa copie...

Erol TEPELI

Relie-F asbl



