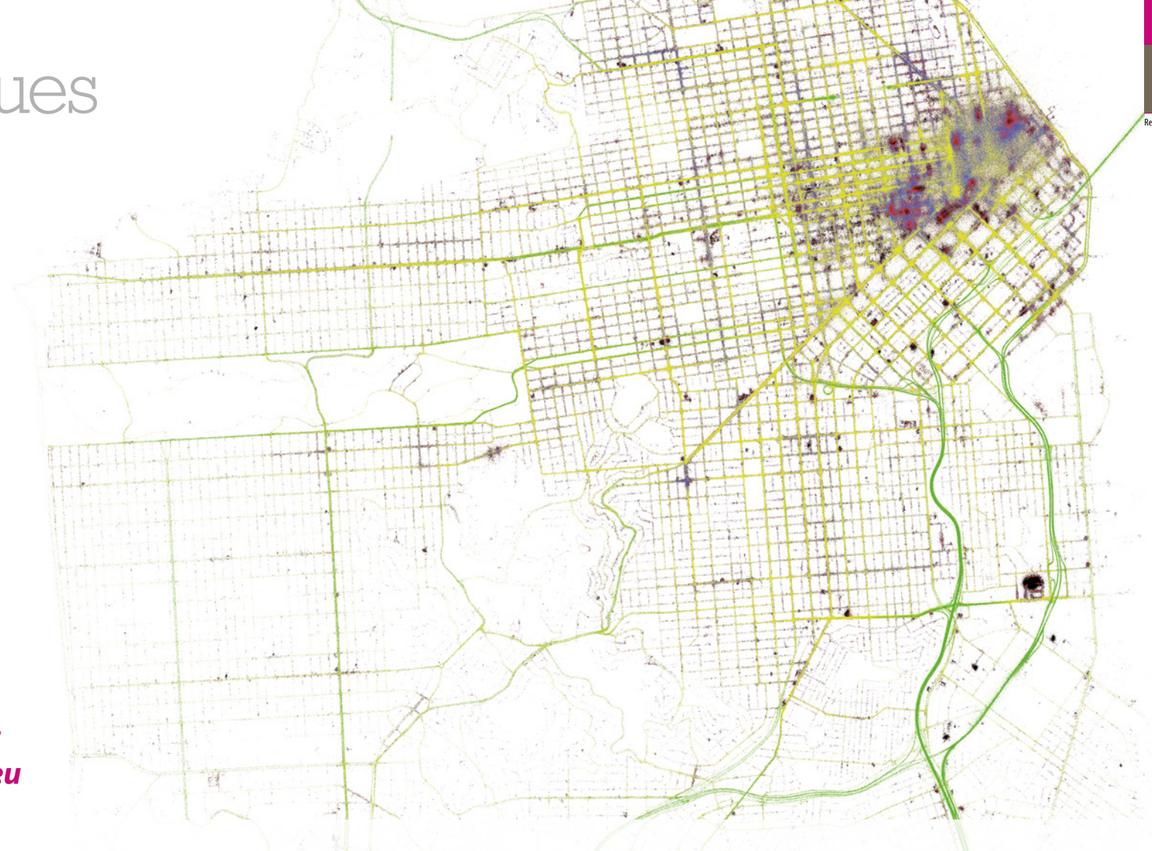
société & vie publique



Repérage des vitesses des taxis à San Francisco, étude de 2008, document Eric Fisher, via Flickr

La recherche pour défendre nos vie privées

Protéger ses données personnelles sur un téléphone mobile

La protection des données personnelles dans la téléphonie mobile est très complexe et ne peut être d'ordre technologique. La cyberassurance reste limitée au domaine professionnel et seules des actions de sensibilisation permettent à ce jour de faire prendre conscience à l'utilisateur des risques encourus.

Ludovic de Carcouët Directeur chez Digitemis

« dans ce monde ultraconnecté et ouvert, la protection des données personnelles est devenue un enjeu important »

Le secteur de la téléphonie et celui des données personnelles sont des domaines très mouvants, où les avancées technologiques sont quotidiennes. L'essor de nouvelles applications (par ex.: *Pokémon Go*), de nouveaux modes de communications (par ex.: *Snapchat*), voire de nouveaux modèles économiques (par ex.: Uber), rendent la protection des données personnelles, liées à ces nouvelles technologies, très complexe. Et la tendance ne s'oriente pas vers une stabilisation du marché.

Dans ce monde ultraconnecté et ouvert, la protection des données personnelles est devenue un enjeu important. La renommée de *Telegram*, cette application qui propose à ses utilisateurs un chiffrement de ses communications, en est la parfaite illustration, malgré son utilisation controversée. La polémique, concernant l'accès aux données de terminaux iPhone de terroristes aux États-Unis, est une autre illustration de la complexité de cet enjeu. En termes de données personnelles, les notions de *protection* et de *confidentialité* peuvent être également remises en cause lorsque les données sont hébergées à l'étranger, impliquant donc la confrontation de plusieurs législations internationales en cas de litige.

Trois menaces pour l'utilisateur

Partant de ces problématiques globales, nos travaux de recherche ont été circonscrits aux problématiques des usages individuels et nous avons ainsi identifié trois types de menaces majeures pour un utilisateur de *smartphone*.

Une des premières menaces est **celle issue des réseaux et des connexions**, qui, face au besoin de l'ultraconnectivité, rend notre terminal mobile vulnérable aux attaques extérieures. Comment sécuriser sa maison si nous laissons nos fenêtres et portes grandes ouvertes ? Ici se pose donc la dualité entre le tout ouvert et la pleine maitrise de la transmission de ses données.

Une autre menace réside dans **les applications ou les systèmes d'exploitation** que nous installons sur nos mobiles. Quelle confiance pouvons-nous avoir envers ces services bien souvent gwratuits auxquels nous fournissons gracieusement notre localisation, l'accès à nos photos ou voire même la gestion de fonctionnalités de notre *smartphone* (appareil photo, liste des appels, microphone, écriture de SMS…). Comment répondre à un besoin, souvent immédiat (nouvelle application, géolocalisation…) et conserver le contrôle de sa vie numérique ?

Il convient d'ajouter **la menace de l'utilisateur lui-même** qui, par distraction, va égarer son téléphone dans le train, rendant ainsi accessible à un tiers une grande partie de sa vie numérique. Ou encore un individu, qui va se connecter sur sa messagerie électronique, dans un terminal aéroportuaire public et oublier de se déconnecter. L'utilisateur, lui-même est une menace importante pour sa propre vie numérique, et ici encore la question du tout accessible et de la centralisation de sa vie numérique peut être remise en cause.

Via ces exemples récents, ainsi qu'à travers nos études approfondies, nous constatons qu'**aucune solution technique ne s'impose** afin de sécuriser ses données personnelles : cela implique également des problématiques éthiques et morales. Malgré ces limitations globales et les menaces individuelles, nous nous sommes penchés sur les solutions d'aide et d'accompagnement de l'utilisateur dans la sécurisation de sa vie numérique.

« ce type de sensibilisation contribue à une prise de conscience de la nécessaire protection de sa vie numérique et replace l'utilisateur comme acteur et décideur »

Digitemis

La société Digitemis réunit des ingénieurs en cybersécurité et des juristes spécialisés dans la protection des données personnelles. Qualifiée Passi (Prestataire d'audit de sécurité des systèmes d'information) par l'Anssi et bénéficiant de 6 labels de la Cnil, elle a été valorisée en 2017 par le Premier ministre Edouard Philippe lors de la remise du *Pass French Tech*.

Pour en savoir plus : www.digitemis.com

Pédagogie et responsabilisation de l'utilisateur

Afin de couvrir ces menaces nouvelles, le marché de **la cyberassurance** reste principalement dédié au monde professionnel pour des raisons de valorisation et d'accessibilité financière. Une donnée professionnelle peut être par exemple valorisée en jour/homme, à l'inverse des données personnelles, pour lesquelles il devient plus difficile de valoriser une photo prise par quelqu'un. Une photo d'un chien n'aura pas la même valeur pour son propriétaire, que pour une personne lambda. À titre d'exemple, si nous comparons la valorisation des données d'un compte *Whatsapp* rapporté à son prix d'achat par Facebook, les données seraient valorisées à 30 $ pour chaque utilisateur.

Nous observons donc des écarts considérables concernant la notion de valeur d'une donnée personnelle, selon les différents points de vue, ce qui laisse à penser que le risque est encore trop récent afin de pouvoir être couvert par des offres de cyberassurance à destination des particuliers.

Cependant la solution immédiate ne réside peut-être pas dans la cyberassurance, et des moyens alternatifs peuvent être imaginés afin d'atteindre la maturité nécessaire aux cyberassurances. Au travers de notre étude complète, nous avons pu démontrer l'efficacité d'une action afin de réduire les risques liés aux vols de données personnelles : la sensibilisation. Plus que jamais, une image a plus de poids que les mots, et la sensibilisation personnalisée a le grand avantage de pouvoir adresser directement et individuellement chacun d'entre nous. Avec l'application *LoupApps*[1], chaque utilisateur analyse, à son échelle, l'utilisation de ses données personnelles par l'ensemble des applications présentent sur son *smartphone*. Ce type de sensibilisation contribue à une prise de conscience de la nécessaire protection de sa vie numérique et replace l'utilisateur comme acteur et décideur, au coeur de son univers connecté. Savoir que Facebook peut accéder au contenu des messages envoyés à mes parents, ou puisse consulter mes photos, ou même prendre des photos sans mon intervention, peut paraître beaucoup plus intrusif et éducatif lorsque cette possibilité est illustrée par la photo de mon chien, ou mon dernier SMS plutôt qu'une simple liste théorique.

Grace à des alternatives comme *LoupApps* l'utilisateur peut prendre conscience des risques encourus pour sa vie numérique, et ainsi en limiter et contrôler sa diffusion.

À noter que les récentes mises à jour d'Android (possibilité de personnaliser les autorisations accordées aux applications), ou encore l'éclosion d'applications telles que *LoupApps*, semblent indiquer la prise en considération de ces problématiques. Elles accordent aux utilisateurs davantage de droits sur le contrôle de leur vie numérique. Cependant cela n'est pas suffisant et ne permet pas de sensibiliser l'utilisateur aux bonnes pratiques. Alerter, sensibiliser, former et guider les utilisateurs dans la gestion de leur vie numérique afin de pouvoir en préserver l'intimité, reste un défi d'actualité. □

1. Cf. www.digitemis.com/outils-cybersecurite-juridique/loupapps/