

Chouchoutez vos applications mobiles comme vos logiciels propriétaires !

Une société jetable

Internet est le reflet de la société de consommation, une société jetable. La multiplication des offres et la concurrence très vive poussent les opérateurs à proposer des produits dotés de performances techniques très importantes, mais ayant une durée de vie réduite. Lorsque l'on se penche sur l'Internet mobile, la situation est évidemment identique. Depuis le lancement de la première génération d'iPhones, les développeurs ont créé un large éventail de produits logiciels, caractérisés par leur ergonomie et leur facilité d'utilisation, principalement destinés à simplifier la vie ou à divertir : les applications mobiles.

A l'image des autres produits contemporains, les applications mobiles sont souvent des produits jetables. Elles sont éphémères et la plupart sont disponibles gratuitement. De nombreux éditeurs de logiciels ou de jeux vidéo développent des applications mobiles dans le simple but de figurer dans les catalogues d'applications propres aux différents smartphones, poursuivant ainsi une stratégie de communication. En septembre dernier, Apple a publié ses nouvelles lignes directrices d'examen préalable des applications (App Store Review Guidelines) en vue de pousser les développeurs à créer des applications plus utiles et plus durables. A cette occasion, la société de Cupertino a fait une déclaration peu élégante mais néanmoins pleine de sens : « Il existe plus de 250 000 applications dans l'Apple Store, nous n'avons plus besoin de simulateurs de pets. »

Protection des données

Les applications mobiles sont particulièrement faciles à télécharger, installer et utiliser. De fait, beaucoup de personnes collectionnent les applications dans leur smartphones simplement pour se targuer du fait de posséder la dernière application futile. Ces personnes ne sont en revanche pas nécessairement conscientes que les applications mobiles peuvent permettre de rassembler un grand nombre d'informations sur les utilisateurs sans que ces derniers ne s'en rendent compte (notamment parce que les sociétés qui exploitent les applications ne disposent pas de conditions générales adéquates, ou simplement parce les utilisateurs ne lisent en pratique jamais les conditions générales d'utilisation). Les applications requièrent fréquemment la création d'un compte utilisateur et peuvent avoir accès à de nombreuses données personnelles, comme la liste de contacts du téléphone, le nom d'utilisateur et le mot de passe, les données de géolocalisation, les habitudes de consommation de l'utilisateur etc. L'utilisation des applications mobiles implique l'acceptation préalable des conditions générales d'utilisation et l'expression de son consentement à chaque fois que des données de géolocalisation sont requises.

Paradoxalement, même si les applications mobiles ont une courte durée de vie, ce n'est pas le cas des traces laissées sur Internet par les utilisateurs. En effet, beaucoup d'applications mobiles impliquent le traitement de données personnelles pour de multiples raisons : la création d'un compte utilisateur, la constitution de bases de données client/utilisateur, l'amélioration des services fournis etc. En sus des exigences

relatives au traitement des données, les données peuvent être utilisées dans de nombreux autres contextes, et notamment à des fins commerciales (envoi d'offres commerciales, de lettres d'information etc.). Elles peuvent tout aussi bien être transférées à un tiers qui les utilisera pour ses propres activités commerciales.

Les règles applicables à la protection des données personnelles sont établies depuis longtemps en France, puisque la première loi en la matière remonte à 1978 (loi Informatique et Libertés) et est extrêmement protectrice des personnes. La violation des dispositions légales relatives au traitement des données personnelles est un délit passible d'une amende pouvant atteindre 300 000 euros par infraction constatée, et d'une peine de prison pouvant aller jusqu'à cinq ans. En outre, la Commission nationale de l'informatique et des libertés (CNIL) a le pouvoir d'adresser des avertissements et d'imposer des sanctions pécuniaires à hauteur de 150 000 euros. La CNIL reçoit un nombre important de plaintes et réclamations et fait régulièrement usage de son pouvoir de sanction. C'est la raison pour laquelle il y a très peu de décisions de justice prononçant des condamnations pénales.

Nous avons déjà insisté sur la nécessité de se protéger sur le plan juridique et technique avant de développer des activités en ligne ou de recourir à des services de cloud computing.¹ La protection des données numériques est particulièrement importante dans la mesure où les sociétés qui collectent les données et les responsables du traitement doivent garantir un niveau optimal de protection technique et apporter des garanties juridiques aux personnes concernées par le traitement. A titre d'exemple, les utilisateurs doivent consentir à l'utilisation de leurs données

¹ Voir notre article « Envoyez vos données dans les nuages, mais gardez-les pieds sur terre! » et notre podcast « security breach ».

personnelles et disposent d'un droit d'accès et de rectification de leurs données.

L'utilisation de données personnelles collectées sur Internet n'est donc pas interdite, à condition que les personnes concernées aient donné leur accord et qu'elles aient été informées de l'utilisation prévue de leurs données. Elles doivent en particulier être informées de :

- La nature des données collectées,
- La raison de leur collecte,
- Toute utilisation prévue de leurs données,
- La façon d'exercer leur droit d'accès, de rectification et de suppression,
- La localisation des serveurs de stockage,
- L'existence d'un transfert de leurs données,
- La durée du stockage.

La protection des consommateurs est considérée comme une priorité en Europe et la protection des données personnelles répond exactement à la même logique. A ce jour, il n'existe pas de cas de sanction relatif à l'utilisation illégale de données collectées lors de l'utilisation d'applications mobiles. Toutefois, la CNIL a publié sur son site Internet en juin ses préoccupations et recommandations au sujet de l'utilisation des smartphones et de la collecte de données lors de l'utilisation de services de téléphonie mobile, en particulier en ce qui concerne les données de géolocalisation.

Exigence en matière de licence

Les applications mobiles sont des logiciels propriétaires. En ce sens, elles doivent être protégées au titre d'un contrat de licence spécifique. Quand bien même l'application ne serait qu'une simple interface mobile permettant aux utilisateurs d'avoir accès à une plateforme Internet au moyen de laquelle une société fournit ses services,

elle devrait néanmoins être protégée contre toute utilisation, reproduction, modification, sous-licence ou vente. Le contrat de licence utilisateur final applicable à l'utilisation de la plateforme Internet ne couvre pas l'utilisation de l'application mobile. Si les développeurs et les sociétés éditrices de logiciels suivent les recommandations d'Apple et proposent des applications mobiles plus durables, une telle protection s'avérera déterminante puisque la concurrence entre les applications ira nécessairement en s'accroissant.

Illustration judiciaire

A ce jour, il n'y pas encore eu d'action judiciaire exercée en France sur le fondement de la violation des règles en matière de protection des données personnelles eu égard à l'utilisation d'applications mobiles. Cependant, comme nous l'avons rappelé plus haut, la CNIL a exprimé des préoccupations et sera à n'en pas douter extrêmement vigilante à ce sujet. La première illustration judiciaire notable est très récente et a été initiée aux Etats-Unis.

Le 23 décembre 2010, une action a été intentée devant la Cour de district (District Court) de Californie contre les sociétés Apple Inc., Pandora media Inc., Backflip Studios Inc., The Weather Channel Inc., Dictionary.com LLC, Outfit7 Ltd., Room Candy Inc. and Sunstorm Interactive Inc. L'action est fondée sur l'utilisation de l'UDID des utilisateurs. L'UDID est un numéro de série assigné par Apple à chaque smartphone produit. L'UDID est comparable à l'adresse IP, le numéro identifiant les ordinateurs sur Internet, sauf qu'il ne peut y avoir qu'un seul UDID par smartphone. Par ailleurs, l'UDID permet une traçabilité du téléphone et est en ce sens également comparable aux cookies utilisés par les publicitaires pour suivre les activités des utilisateurs en ligne.

En France, l'adresse IP n'est pas considérée comme une donnée personnelle, selon un jugement de la Cour d'appel de Paris², au motif qu'elle ne permet pas d'identifier directement les personnes. En France, ce sujet est très discuté dans la mesure où tous les régulateurs européens considèrent l'adresse IP comme une donnée personnelle et la CNIL a également exprimé son désaccord vis-à-vis du jugement de la Cour d'appel de Paris.

Le procès intenté aux Etats-Unis est une Class Action exercée au nom des personnes propriétaires d'iPhones qui ont téléchargé les applications fournies par les défendeurs. L'assignation allègue que les applications exploitées par les défendeurs avaient accès à l'UDID des demandeurs et à leurs données de géolocalisation et qu'elles transmettaient ces informations à de nombreuses régies publicitaires. Lorsque ces informations sont associées à d'autres types d'informations collectées lors de l'utilisation des applications par les utilisateurs (les habitudes de consommation des utilisateurs par exemple), elles deviennent en effet de précieux outils commerciaux au bénéfice des régies publicitaires.

Cette action judiciaire fait suite à plusieurs études et articles rapportant que les applications mobiles favorisent la violation des règles applicables à la protection des données personnelles.³ Même si cette

² CA Paris 13^{ème} chambre Section B du 27 avril 2007 et CA Paris 13^{ème} Chambre Section A du 15 mai 2007

³ Eric Smith *iPhone Applications & Privacy Issues: an Analysis of Application Transmission of iPhone Unique Device Identifiers (UDID's)*, 1^{er} octobre 2010, disponible sur <http://www.pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf> ; Scott Thurm et Yukari Iwatani Kane *Your Apps Are Watching You*, 18 décembre 2010 publié dans le Wall Street Journal, disponible sur <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>.

affaire n'a pas été jugée, elle est une illustration pertinente de la façon dont la protection des données personnelles peut être hypothéquée pour des raisons commerciales. Cela nous remet également en mémoire qu'il faut toujours être extrêmement vigilant lorsque l'on navigue

sur Internet à partir d'un ordinateur ou d'un téléphone portable. Du côté des développeurs et des éditeurs de logiciels, cette action montre combien il est essentiel de disposer d'un cadre juridique protecteur et efficace.

Le 17 Mars 2011

Une synthèse de Diane MULLENEX, Avocat à la Cour – Solicitor England & Wales et de Clément GAUTIER, Avocat à la Cour, Département TMT du Cabinet Ichay & Mullenex Avocats.

Le cabinet Ichay & Mullenex Avocats est spécialisé dans la gestion des problématiques juridiques liées à l'activité des entreprises de nouvelles technologies et de développement durable. Il conseille ainsi de nombreux acteurs du e-commerce, de l'informatique, des médias, des télécoms et de la recherche dans la gestion de leurs affaires au quotidien, pour leurs projets de croissance interne ou externe et leur développement à l'international. L'ensemble des avocats du cabinet Ichay & Mullenex Avocats a reçu une double formation en complétant leur formation française soit par une formation à l'étranger soit par une formation en école de commerce. Chacun d'entre eux est tourné vers la nouvelle économie et la mondialisation des échanges accompagnant leurs clients avec une vision pragmatique de la vie des affaires.

5, rue de Monceau 75008 Paris - France

Tel : +33 1 42 89 19 80

Fax : + 33 1 42 89 14 99

www.ichay-mullenex.fr