Sylvain Métille, docteur en droit, avocat spécialisé en droit de la protection des données et des nouvelles technologies au sein de l'étude id est avocats sàrl à Lausanne, chargé de cours à l'Université de Lausanne (droit pénal informatique) et à l'IIMT à Fribourg (Telecommunications Law et Data Protection Law), blogueur (https://ntdroit.wordpress.com).

sylvain.metille@idest.pro

Confier ses données à une société étrangère n'est pas sans risque

Zusammenfassung In der Cloud gespeicherte Daten werden oft in den USA oder von amerikanischen Firmen gehostet. Dadurch werden die Daten dem amerikanischen Recht unterstellt, und das schweizerische Bundesgesetz über den Datenschutz hat keinen Einfluss. So erlaubt das FISA der amerikanischen Regierung beispielsweise, Daten von Nicht-US-Bürgern von diesen Unternehmen zu verlangen. Folglich sollte jede Person, die über sensible oder vertrauliche Daten verfügt, bei der Wahl des Dienstleistungserbringers auch auf dessen Sitz und Eigentümer achten.

L'informatique en nuage (cloud computing) n'est pas nouvelle, mais elle devient omniprésente dans l'organisation actuelle d'un bureau. Chacun apprécie de pouvoir accéder depuis n'importe où à son espace de travail professionnel, de retrouver en déplacement des fichiers enregistrés «en ligne» ou plus simplement son courrier électronique. On peut accéder à ses documents et autres données en tout temps et depuis n'importe où pour peu que l'on dispose d'un accès à Internet. L'hébergement des fichiers est souvent gratuit ou presque. Cette disponibilité complète induit cependant une certaine perte de maîtrise, à tout le moins physiquement, de ses fichiers qui peuvent contenir des données sensibles. Ils ne sont plus dans un tiroir que l'on ferme à clé et auquel on sait qui a accédé. Cette nouvelle facilité d'accès fait parfois perdre de vue les risques qui peuvent y être liés.

Le cadre légal pose certaines limites au traitement des données, vu l'atteinte à la personnalité que cela peut représenter. En Suisse, la Loi fédérale sur la protection des données (LPD) contient les principes et les conditions à respecter lors du traitement de données personnelles de tiers. La LPD s'applique au traitement de données qui a lieu en Suisse (ATF 138 II 346, consid. 3). La notion de traitement de données est large – elle inclut la collecte, la conservation, la modification, la communication, etc. (art. 3 lit. LPD) – et la LPD pourra s'appliquer à un fournisseur d'hébergement étranger qui propose ses services en Suisse et traite des données en Suisse même s'il ne dispose pas d'une filiale en Suisse ou d'un site Internet exclusivement dédié à la Suisse.

En principe, les lois nationales de protection des données s'appliquent d'abord dans leur pays d'origine. Le projet de nouveau Règlement définissant un cadre général de l'UE pour la protection des données qui devrait remplacer la Directive 95/46/CE prévoit pourtant expressément son application hors de l'UE pour les données concernant des résidents européens.

Déjà aujourd'hui la LPD impose à celui qui traite ou exporte des données dans un pays n'offrant pas le même niveau légal de protection que des garanties particulières soient apportées (par le biais d'un contrat) ou que la personne dont les données sont traitées en soit informée et donne son accord spécifique (art. 6 LPD). Autrement dit cela signifie que soit les données sont traitées avec les mêmes garanties que si elles l'étaient en Suisse ou alors que la personne concernée accepte en toute connaissance de cause que les mêmes garanties ne soient pas offertes. Mais ces garanties ne concernent que le traitement des données qui est fait par la personne (physique ou morale) qui les exporte ou les traite à l'étranger, et n'excluent pas l'application du droit local du pays étranger que cette personne doit respecter, en particulier des lois de procédure civile ou pénale, des lois fiscales, des lois sur la transparence ou encore des lois sur le renseignement. L'entité étrangère peut être tenue de transmettre des informations en application de sa loi nationale, et la LPD suisse ne pourra pas s'y opposer.

Aux USA par exemple, le Foreign Intelligence Surveillance Act américain (FISA) permet au Gouvernement américain d'obtenir facilement des informations concernant des personnes qui ne sont pas des résidents U.S. lorsque les données sont hébergées sur sol américain ou traitées par des entreprises américaines. Le FISA avait initialement pour but de surveiller les espions étrangers, mais au gré des modifications cette loi vise désormais les pouvoirs étrangers et les agents de pouvoirs étrangers, une notion sujette à une interprétation large. L'ACLU, une organisation américaine de défense des libertés individuelles, considère que les avocats, journalistes, chercheurs et universitaires étrangers sont également inclus dans cette notion. Comme les non-résidents U.S. sont exclus de la protection offerte par le IVe Amendement, ils ne bénéficient même pas de la possibilité de saisir une autorité judiciaire ou d'être informé

une fois la transmission de leurs données intervenue. Il existe dès lors un risque réel que des données de ressortissants suisses ou européens puissent être obtenues par les autorités américaines. Les pays membres de la Convention européenne des droits de l'homme garantissent en revanche une protection similaire à leurs ressortissants nationaux et aux étrangers, en particulier le droit de saisir une autorité judiciaire (exigence de l'art. 8 al. 2 CEDH).

La grande majorité des fournisseurs de services d'hébergement sont américains (comme Amazon, Apple, Google, Microsoft, ...). Alors que la quasi-totalité des données américaines sont hébergées aux USA ou par des sociétés américaines, seul un tiers des données du vieux continent sont hébergées en Europe ou par des sociétés européennes. Cela signifie que deux tiers des données européennes sont soumises à des règles étrangères – notamment s'agissant de l'accès aux données par les autorités ou l'obligation de transmettre des informations –, règles sur lesquelles le droit national du pays d'origine n'a aucune influence et que les entreprises américaines doivent et vont évidemment respecter.

Le journaliste soucieux de la protection de ses sources ou simplement celui qui veut éviter qu'un gouvernement étranger n'ait accès à des informations sur ses activités privées ou professionnelles devrait être prudent sur le choix de ses outils de travail, même les plus courants. Le choix d'un fournisseur de services – y compris un simple hébergeur de données ou fournisseur de courrier électronique – dépendra donc d'abord du type de données traitées. Il n'est guère possible de négocier les conditions générales de l'offre standard proposée au grand public, mais on prendra néanmoins garde aux pays concernés, aux possibilités que le fournisseur sous-traite le service et aux conditions d'utilisation. Le choix d'un fournisseur de services local et/ou payant suffit parfois à éviter d'être exposé. Des moyens techniques comme le cryptage des données ou la division des données entre différents prestataires peuvent aussi réduire les risques et peuvent être mis en place indépendamment du fournisseur de services.

A défaut de pouvoir bénéficier d'un environnement technique propre ou renoncer à l'utilisation d'un smartphone qui effectue automatiquement une sauvegarde vers un serveur dont la location est inconnue, l'utilisateur doit au moins garder en mémoire que selon le lieu où se trouveront ses données, un tiers pourra les obtenir légalement – un gouvernement pour des motifs de sécurité nationale, un concurrent dans le cadre d'une procédure judiciaire, une personne concernée pour ses propres données, etc. – et donc tenir compte de ce risque. Celui qui traite des données sensibles ou simplement dont il veut éviter qu'elles ne puissent être consultées doit désormais choisir attentivement ses outils de travail, y compris ceux qui semble les plus banals.

Résumé Les données sauvegardées dans le cloud sont le plus souvent hébergées aux USA ou par des sociétés américaines. Cela expose les données à des lois américaines sur lesquelles la LPD suisse n'a évidemment pas d'emprise. Le FISA permet par exemple au Gouvernement américain d'obtenir les données de non-résidents U.S. de la part de ces entreprises. Celui qui traite des données sensibles ou veut garder ses données confidentielles doit donc faire attention au choix de ses fournisseurs de services et à leur localisation.