Sécurité, vie privée, données personnelles

Évolution historique, état des lieux

Patrick Kineider

Cet article s'inscrit dans la thématique largement développée ces dernières années au sein du Groupe de Travail ADELI «Juridique et Internet du Futur ».
Les socles technique et organisationnel (sécurité des systèmes d'information) et juridique (protection des données «sensibles» ou «personnelles») s'inscrivent à présent dans un nouveau périmètre mondialisé.
Ceci est dû entre autres, à la globalisation des échanges de données informatique et Télécommunications, au développement de sociétés commerciales internationales autour de l'Internet : Google, Apple, Facebook, Amazon., appelés les «GAFA».
Des dispositions sont en cours dans des pays ou groupes de pays pour réguler l'Internet en matière de protection des données sensibles.
Le texte, dont plusieurs références à des documents adéliens sont portées en annexe, a pour finalités de faire le point sur des grandes lignes du sujet, et de tirer quelques perspectives.

Qu'appelle-t-on «donnée sensible»? Définition et enjeux

En général, une donnée informatique est dite « sensible » si un individu n'ayant pas le droit ou l'autorisation législative ou réglementaire d'y accéder, crée en le faisant, vis-à-vis du (ou des) « propriétaire(s) » de ces données un risque de préjudice (moral, financier, crapuleux...) ou un préjudice avéré.
Les données nominatives constituent le type même de donnée sensible. Exemples de telles données : le nom; le numéro de compte bancaire; le numéro national de sécurité sociale.
Les risques généraux concernant les données sensibles sont les suivants :

- la malveillance consistant à se faire passer pour un autre (usurpation d'identité) ;
- le traçage individuel par les informations de localisation (triangulation des mobiles, fichiers GPS...) ;
- l'accès à des informations telles que la religion, l'appartenance politique, les goûts et l'exploitation publique, ou politique, ou commerciale de toutes ces informations (entrave aux libertés fondamentales, fraude administrative, escroqueries, abus de confiance divers).

Évolution historique

Technique et organisationnel : l'évolution de la sécurité des systèmes d'information

Avant 1995, dans les établissements publics et les diverses sociétés commerciales et industrielles, les données dites sensibles étaient gérées au sein de systèmes d'information protégés et seulement accessibles à un personnel habilité.

Dans chacune de ces structures, la mise en place et la coordination non seulement des procédures techniques, mais de l'information et de la formation des services et des salariés, a été progressivement confiée à un Responsable Sécurité du Système d'Information. Il est de nos jours, le plus souvent rattaché à la Direction de l'entreprise, de l'unité ou du service. En France, la Sécurité des SI obéit à diverses normes, en particulier l'ISO 27000.
Une donnée informatique peut être sécurisée (en lecture, modification, suppression) :

- par des codes d'accès, en général l'authentifiant (désignant l'utilisateur) et l'identifiant (précisant son accès au type de donnée). Exemple : numéro et code de carte de crédit ;
- par chiffrement algorithmique, transformant la donnée reconnaissable en chaîne de caractères suivant un algorithme mathématique.

La Sécurité des SI veille à ce que les données et applications soient protégées, et plus la donnée est sensible (compte bancaire, dossier médical, défense nationale), plus le système est susceptible d'être attaqué, donc sa protection est d'autant plus sophistiquée.

Pour la protection des données personnelles, la CNIL est l'autorité de référence. Les données personnelles ou nominatives utilisées sur le plan individuel peuvent également être stockées, soit sur des micros individuels (fixes ou portables, « assistants personnels »), protégés par un couple « identifiant + mot de passe ». À partir de la fin du siècle dernier, grâce à Internet, les échanges d'informations se sont globalisés. Internet relie peu à peu, l'ensemble des utilisateurs de micro-ordinateurs, via des serveurs et des réseaux de télécommunications sophistiqués. L'e-commerce, la e-administration, l'e-éducation se généralisent.

Avant et après Internet, les SI ont constamment été soumis à des attaques extérieures. Les virus, bombes logiques et chevaux de Troie sont de petits programmes malveillants introduits dans un système ou sur un terminal, visant à altérer ou à détourner de l'information, donc en particulier les données personnelles.
Par ailleurs, sur Internet, quelques grandes attaques spectaculaires sont le fait de groupes de hackers très organisés, souvent commandités par des lobbies soit crapuleux, soit politiques (incluant des États eux-mêmes). Ainsi le programme nucléaire iranien fut attaqué en 2010 par des « hyper-virus ».
La gouvernance mondiale d'Internet reste essentiellement américaine.
Vers 1995-2000 apparaît le « téléphone mobile » individuel, suivi du « smartphone » aux fonctionnalités plus larges (Internet, GPS, paiements en ligne, suivi personnel de paramètres médicaux, domotique...). En 2014, dans le monde, le nombre de téléphones mobiles utilisés est de près de 5 milliards d'unités,
Les smartphones, qui se substituent de plus en plus aux micros (précisément en raison de leur mobilité) fonctionnent avec des systèmes d'exploitation spécifiques (IOS, Android). Bien que la Société Trend Micro ait évalué à plusieurs milliers les attaques possibles sur les réseaux mobiles, nous ne disposons pas de statistiques fiables de celles-ci à l'heure actuelle. Depuis plusieurs années, on trouve également les premiers « appareils connectés » en réseau, par exemple la « montre connectée ». Les données mondiales sont théoriquement accessibles par chacun : tout est-il devenu transparent, tout est-il devenu possible ?

Le « monstre » Google : le produit performant mais dangereux par excellence

Née aux États-Unis en 1988, la Société Google est l'une des plus imposantes entreprises du marché commercial d'Internet.
Initialement, c'est un moteur d'indexation et de recherche de documents textes ou multimédias de tous types sur le web Il s'est par la suite diversifié par la création de produits mondiaux tels que (non exhaustivement) : une messagerie en ligne (Gmail) ; plusieurs plateformes multimédias (Drive et YouTube) ; les cartographies terrestres (MAPS et Earth) ; le système d'exploitation mobile Android. Plus récemment la Société Google s'est lancée dans divers projets d'intelligence artificielle médiatisés, considérés comme assez ambitieux, pour ne pas dire utopiques.

Le logiciel « Google Street View » est un sous-produit de l'outil général « Google Maps », cartographie mondiale en ligne. Dans la plupart des pays, sur des axes de communication choisis (autoroutes, grandes routes, rues d'agglomérations), un curseur permet, grâce à l'utilisation pour la création des cartes, de véhicules équipés de photos et de caméras « Google Cars » d'afficher en ligne, des photos : de chaussées, plaques de véhicules, panneaux publicitaires, piétons. On ne compte plus les plaintes pour « droit à l'image » concernant ces individus, ou les numéros d'immatriculation des voitures (que Google a dû griser), etc.

S'agissant du moteur de recherche lui-même, la convivialité de la page d'accueil, la pertinence des critères d'indexation par des mots-clefs judicieusement choisis, ont fait le succès de Google (qui draine 8 % de l'activité web à lui tout seul avec 1 000 milliards de pages web indexées en 2008). Le « business model »de Google est le suivant : les entités lui fournissant des mots-clefs le financent par une publicité ciblée ; mais une conséquence dangereuse est que les recherches quasi quotidiennes d'un internaute sur Google permettent de le tracer son adresse IP sur le web Toile, au début sans aucune garantie.

Ces dernières années, l'État américain ainsi que la CNIL française, puis les instances de l'Union européenne, sont entrés dans une période de « négociations-sanctions » à l'égard de la firme californienne.
En 2009, Google est astreint à payer 300 000 euros de dommages et intérêts à deux éditeurs pour avoir reproduit intégralement et en les rendant accessibles, des extraits d'ouvrages sans l'autorisation des ayants droit ;

- en 2010, Google est condamné en France pour le délit de « diffamation par algorithme » pour avoir associé certains mots-clés avec les termes sensibles tels que « viol » ou « condamné » ;
- en 2011, Google préfère payer une amende de 500 millions de dollars aux autorités américaines, plutôt que d'être poursuivi par la justice pour avoir fait la promotion de médicaments illégaux ;
- en 2014, après une condamnation de la CNIL à 150 000 euros pour ne pas respecter la protection des données nominatives, Google met en place sur son site, un « formulaire de droit à l'oubli ».

Avec Google, dont on peut difficilement se passer, les autorités nationales et internationales, ne sont pas au bout de leurs peines !

Données personnelles : situation française

Textes nationaux

Les 4 principales lois informatiques françaises dans le domaine de la sécurité et de l'éthique des SI sont :

- en 1978, Informatique et Libertés (protection des données personnelles), relayée par les « CIL » (correspondants spécialisés dans les structures administratives ou commerciales) et plus récemment :
  - les lois HADOPI et HADOPI2 (protection des droits d'auteurs),
  - la « loi sur la confiance dans l'économie numérique » (responsabilité des hébergeurs),
  - la LOPPSI et la LOPPSI2 (traçage des sites subversifs ou anti-éthiques, de tous ordres).

Elles sont présentées, dans leurs grandes lignes et finalités, dans l'ouvrage « Conformité Légale des SI » édité en 2011, dont le lien figure en annexe.

Le bilan de la 1e Loi après 36 années d'existence, au plan des questions juridiques résolues, de l'édiction de normes, de régulation des échanges en général, de chef de file des tentatives de protection européenne des données est particulièrement à saluer.

Cas de la vidéosurveillance (encore appelée : vidéoprotection)

Il s'agit de dispositifs de caméras et de transmission d'images numérisées, situés dans des espaces, soit publics, soit privés, et permettant une surveillance à distance par une autorité habilitée :

- les forces de l'ordre nationales ou municipales pour l'espace public ;
- des sociétés de surveillance dans les espaces privés, en particulier les logements individuels.

En 2014, le nombre de caméras « autorisées » du premier type, dans l'espace public, est estimé à un peu moins d'un million. Les données numérisées sur leurs supports finals, en particulier les images photographiques et filmées, sont sensibles.

La vidéosurveillance rencontre deux problèmes de fond :

- son efficacité quant à l'aide à la sécurité publique est loin de faire l'unanimité (en fait, elle est considérée par beaucoup de collectivités locales comme un simple soutien à l'action des forces de l'ordre) ;
- et surtout, de nombreuses voix s'élèvent contre les possibles atteintes à la vie privée en cas de réutilisation des images à des fins personnelles, professionnelles (flicage des salariés), commerciales, politiques, etc. Les jurisprudences françaises en la matière sont nombreuses.

Attentats terroristes de janvier 2015

À la suite des attentats terroristes de Janvier 2015, un important ensemble de mesures policières et judiciaires a été annoncé par le gouvernement français, dont un volet significatif consiste dans la «surveillance des sites et connexions à but terroriste» sur Internet.

Les moyens proposés à ce jour sont :

1. poursuites judiciaires contre les sites faisant l'apologie du terrorisme, ou blocage administratif provisoire de ces sites ;
2. fermeture définitive sur décision de justice ;
3. création de « contre-sites » pédagogiques pour les jeunes, expliquant les dangers du terrorisme tels : www.stop-djihadisme.gouv.fr.

Comme cela a été le cas pour la loi HADOPI, les organismes de défense de la liberté sur le Web s'élèvent déjà contre l'efficacité relative des mesures de blocage, arguant du contournement facile par les terroristes; ils défendent en revanche les actions d'information.

Cas des réseaux sociaux individuels sur Internet

Ce sont de gigantesques serveurs internationaux permettant à l'utilisateur final, à travers un profil individuel, de définir un certain nombre d'interlocuteurs privilégiés, et d'engager soit des discussions « texte », soit des échanges multimédias (images, films sonores ou pas). Actuellement deux réseaux sociaux à finalité générale devancent très largement les autres en nombre d'utilisateurs et volumes de données échangées et stockées : Facebook et Twitter, tous deux issus des USA il y a une quinzaine d'années.

La faille sécuritaire des réseaux sociaux, amplement décrite dans plusieurs de nos publications, consiste dans la « porosité » des données saisies par le titulaire d'un profil.

Car celles-ci peuvent être vues et réutilisées par des individus n'ayant pas en en connaître, à des fins commerciales, voire crapuleuse ou subversive dans un petit nombre de cas.

Si on prend le cas de Facebook, sur le site officiel on lit dans la rubrique « confidentialité » : « une entreprise ou une organisation peut vous atteindre en demandant à Facebook de diffuser ses publicités aux personnes qui ont utilisé ses sites web et ses applications en dehors de Facebook. Par exemple, vous pouvez consulter le site web d'une entreprise qui utilise des cookies pour enregistrer ses visiteurs. L'entreprise demande ensuite à Facebook de diffuser sa publicité à cette liste de visiteurs et vous pouvez voir ces publicités sur Facebook comme sur d'autres sites. Il s'agit d'un type de publicité personnalisée. ». Belle information commerciale, mais pas vraiment de nature à défendre nos données contre les ingérences !

En France, le MEDEF, l'APEC, le SYNTEC et plusieurs autres « acteurs de l'emploi » ont récemment signé une convention de partenariat pour promouvoir une charte sur le bon usage des réseaux sociaux dans les procédures de recrutement. Elle vise à sensibiliser les employeurs, les cabinets spécialisés et les candidats, par exemple sur la recommandation de ne pas utiliser les moteurs de recherche ni les réseaux sociaux comme outils d'enquête, afin de préserver la protection de leurs données personnelles.
Concernant les réseaux sociaux en entreprise, à finalités spécifiques, qui posent des problèmes de sécurité spécifiques à ces entités, se référer à l'article ADELI de 2014 (lien en annexe)

Cloud computing
Le « cloud » - en anglais « nuage informatique » - est une architecture distribuée, par laquelle des individus ou des entités (entreprises, etc.) centralisent leurs données chez un fournisseur unique garantissant une puissance de calcul supérieure à celle d'un traitement local.
Des données éventuellement sensibles étant ainsi délocalisées, la question de la sécurité de leurs accès se pose.
Par exemple, un des opérateurs de téléphonie mobile dispose d'un cloud, où un client peut poster un document en contrôlant les accès extérieurs, par exemple en envoyant le lien du document à la boîte de courriel, personnelle de l'utilisateur concerné, ainsi habilité par le propriétaire.
Une certification de sécurité des « clouds » européens est en cours de validation fin 2014 : la « Cloud confidence »

Big data
On désigne ainsi, des ensembles de données importants (pouvant se compter en « téraoctets » soit 10 puissance 12 octets). Ils concernent par exemple, un domaine technique (processus industriel), économique (banque, assurance), environnemental (météorologie) ou autre (médical).
Les réseaux sociaux génèrent de gros volumes de big data de toute nature (30 milliards de données en 2013).
Les USA, l'UE font progresser les technologies des big data. Une des architectures ad hoc est constituée par le Cloud.
Parmi les données du big data, celles qui sont publiques sont regroupées sous l'appellation « Open data » (données accessibles), par exemple, les statistiques administratives et géographiques.
Il semble qu'une grande partie de la sécurité des clouds techniques et économiques soit, dans les années à venir, dévolue aux entreprises.
La référence de l'article ADELI « introduction et enjeux du big data » se trouve en annexe.

Positions de principe de l'UE

Depuis 2012, l'Union européenne, sous l'impulsion toute particulière de la CNIL française, a créé un « Groupe de réflexion de l'Article 29 « G29 » par référence aux articles 29 et 30 de la Directive 95-46-CE, sur la protection des données. Ce groupe a élaboré une déclaration commune ayant valeur de charte, dont la référence ADELI se trouve en annexe.
D'ores et déjà, des compléments à la charte sont prévus, concernant les smartphones et plus généralement les « objets connectés ».
Positions de principe des États-Unis : des situations contradictoires.
Dans les années 2010, deux informaticiens, l'Australien Julian Assange et l'Américain Edward Snowden, ont défrayé les médias par des actions personnelles spectaculaires :

- concernant J. Assange, ce sont des révélations sur certaines procédures diplomatiques des États-Unis ;
- concernant E. Snowden, il s'agit d'ingérences des Agences d'État et des organismes de sécurité intérieure américains (CIA, FBI, NSA..) vis-à-vis du contenu des communications téléphoniques et courriel, de citoyens.

À l'heure actuelle, les États-Unis ne disposent pas d'un socle juridique de protection des données personnelles tel que la CNIL en France.
En revanche, ils privilégient, au nom d'une supposée « raison d'État », renforcée jusqu'à l'excès après les événements du 11 septembre 2001, la faculté pour les services publics américains de surveiller, sinon tous, du moins certains échanges personnels « supposés » avoir des fins subversives.
En sens inverse, en 2013 et 2014, des ingérences avérées de la NSA non seulement dans des fichiers d'entreprises européennes en lien avec l'armement, mais aussi, dans certaines communications téléphoniques de dirigeants politiques eux-mêmes, ont conduit divers pays d'Amérique du Sud et de l'Union européenne, à prendre en la matière des mesures de protection diverses ; dont l'efficacité n'a d'ailleurs pas été prouvée.
Deux textes juridiques – non exhaustivement – existent en matière de données personnelles aux USA :

- le « Privacy Act » de 1995 interdisant à des organismes rattachés à des États extérieurs, ou à des entités réputées adeptes des libertés les plus étendues sur le NET, à accéder à certains fichiers ;
- le « Patriot Act » de 2001, qu'on pourrait traduire par « loi de sécurité nationale destinée à protéger l'État Américain d'individus ou d'organisations défendant exagérément certaines libertés d'expression et d'échanges ».

Cas particulier de la zone « Asie Pacifique »

Dans la plupart des pays démocratiques, les multinationales GAFA tentent de s'implanter peu à peu, conduisant à un développement des connexions à Internet depuis des ordinateurs ou des smartphones. Deux pays asiatiques émergents présentent deux panoramas assez différents.

La Chine

Avec 1,6 milliard d'habitants, dont près de la moitié d'internautes, ce pays est devenu la 1ère économie du monde quant au taux de croissance, la production, les réserves financières, le développement des classes moyennes, mais au sein d'une organisation politique demeurée historiquement très étatique, avec des libertés démocratiques assez réduites.

En particulier, les connexions à Internet sont contrôlées par des dispositifs de filtrage, par exemple concernant Google (constamment en conflit avec l'État chinois), Yahoo et la société de télécommunications CISCO.

De fait, la Chine développe en interne des outils tels que des réseaux sociaux nationaux We-Chat et Q-Zone, avec des règles du jeu fortement contrôlées et régulées par l'État.

L'Inde

Avec une population du même ordre (1,2 milliard d'habitants, 400 millions d'internautes), ce pays est beaucoup plus ouvert que le précédent, en raison d'une démocratie plus affinée, et d'infrastructures universitaires et de recherches puissantes (300 000 ingénieurs locaux, transferts de technologies, etc..).

De fait, en particulier, la pénétration des GAFA et du Web 2.0, y est plus puissante qu'en Chine.

Conclusion, perspectives

Le panorama général que nous avons réalisé indique deux tendances a priori contradictoires :

- la banalisation globale de l'Internet et des télécommunications, largement dans le monde euro-américain, plus lentement dans les autres pays, et qui entraine un accès immédiat et de qualité du citoyen à nombre de données de tous ordres, par exemple les Open data ;
- à la suite de nombreux risques et abus lors de la montée en puissance des outils et de l'activisme de certains États, seule l'Union européenne tente, non sans difficulté, de développer de la façon la plus homogène possible sur le continent, un semblant de « régulation ».

Pour conclure, une note philosophique.

L'écrivain et penseur anglais du siècle dernier H.G. Wells, s'exprimait ainsi en 1945 : « L'esprit n'est plus capable de s'adapter assez vite à des conditions qui changent plus rapidement que jamais, car nous sommes en retard de cent ans sur nos inventions »

En matière de données personnelles numérisées, 70 ans plus tard, il m'apparaît plus raisonnable de penser qu'après les errements des premières années, à terme, la force de l'esprit humain et de l'organisation collective finira par s'imposer et rendra l'ensemble plus « secure », pour reprendre un néologisme anglais, bref plus « humanisé » !▲

patrick.kineider@hotmail.fr

ANNEXE - Références adéliennes

Thème et lien du site ADELI	Parution
Au sujet du C.I.L : http://www.adeli.org/billet/nouveau-statut-du-cil	2010
Document ADELI « conformité légale des SI » http://www.adeli.org/contenu/conformité-légale-des-si-louvrage	2011
La CNIL et Google : http://www.adeli.org/billet/rapport-cnil-sur-nouvelles-regles-de-confidentialite-google	2012
Introduction et enjeux du big data : http://www.adeli.org/contenu/lettre-88-été-2012-data	2012
Articles de la Lettre d'ADELI Lettre 96 été 2014 -confiance-numérique	2014
Déclaration commune des autorités européennes de protection des données http://europeandatagovernance-forum.com/pro/fiche/quest.jsp; jsessionid = vRxcqlgdI0ULOP5iUtbCvdMX. gl1 2014	