

La protection internationale des données personnelles sur l'internet

La Commission juridique de l'Isoc France vous propose cette note dans un but uniquement pédagogique. Si vous avez un besoin précis, consultez un professionnel.

Introduction

En s'inscrivant sur des listes d'échanges, en s'abonnant à un service, à des sites de réseaux sociaux ou en faisant un achat en ligne, l'internaute fournit sur lui-même des informations que d'autres ne manqueront pas d'exploiter à des fins commerciales ou autres.

Par sa navigation sur les sites qu'il consulte, il laisse également des traces, sans en avoir nécessairement conscience, notamment des données techniques telles que son adresse IP. Il est alors possible d'identifier les dates et heures de connexion, les thèmes de consultation (ex : site de santé, sites politiques...).

L'internaute donne ainsi volontairement ou involontairement de multiples renseignements privés sur le réseau.

Ces informations sont appelées données à caractère personnel car elles permettent d'identifier directement ou indirectement une personne physique (nom, prénom, adresse, date de naissance, etc.). Ces données permettent la constitution de profils dont l'utilisation peut parfois porter atteinte aux droits et libertés de la personne.

La recherche d'un juste équilibre entre respect de la vie privée, intérêts mercantiles et besoin de conserver des traces pour identifier des comportements délictueux est délicate. En France, la loi Informatique et Libertés et quelques autres textes réglementent la collecte, la conservation et l'exploitation des données personnelles. Le non-respect de cette réglementation peut être ainsi sanctionné par le juge mais aussi par l'autorité administrative indépendante qu'est la CNIL.

Cependant, au-delà de ce cadre législatif national et face à un réseau de dimension mondiale, qui protège les internautes ?

Auteur (s): Michèle Bruniaux, pour la commission juridique.

1. Les textes qui vous protègent au niveau européen

Les organisations internationales, et surtout européennes ont manifesté leur volonté d'assurer le respect de la vie privée et la protection des données personnelles, notamment des internautes.

Les initiatives européennes ont pour but d'amener tout les Etats de l'Union Européenne à harmoniser leurs législations nationales, c'est-à-dire à assurer un même niveau de protection juridique minimale pour tous à travers l'Union.

Les textes les plus importants sont la Directive 95/46/CE du 24 octobre 1995 relative à la protection des données personnelles que la France a transposée par la loi du 6 août 2004, et la Directive « vie privée et communications électroniques » du 12 juillet 2004 transposée par la loi du 21 juin 2004 relative à l'économie numérique. Les pays de L'union Européenne ont tous transposé dans leur droit national la Directive 95/46/CE, et accorde ainsi une protection équivalente.

Le Conseil de l'Europe a également adopté plusieurs recommandations, et élaboré une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

2. Les textes qui vous protègent au niveau international

La situation est plus disparate dès qu'on sort de l'Union européenne. Une résolution adoptée par l'assemblée générale des Nations Unies en 1990 a interdit la collecte et le traitement des données à caractère personnel selon des moyens illicites ou déloyaux. Elle garantit une protection minimale des droits de l'homme dans ce domaine, notamment concernant les données dites sensibles.

L'OCDE, organisation internationale à vocation économique, a émis en 1980 une recommandation comportant des lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données.

L'OMC qui s'occupe du commerce international a également pris position pour la protection de la vie privée des personnes ainsi que pour la protection du caractère confidentiel des dossiers.

Toutefois, aucune de ces dispositions ne sont obligatoires. Elles traduisent, cependant, un consensus international et servent de fondements pour l'élaboration des règles de protection de la vie privée au niveau mondial.

3. La protection des données sensibles

Les données sensibles sont les informations faisant apparaître directement ou indirectement les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales des personnes, les informations relatives à la santé ou à la vie sexuelle. En France, par exemple, la collecte de ces données est interdite, et doit faire l'objet de dérogations auprès des instances de contrôle telle la CNIL pour être exceptionnellement autorisée.

4. Que se passe-t-il lorsque des données personnelles sont transférées d'un pays à un autre ?

Une personne qui traite des données personnelles peut décider de les transférer à l'étranger. La situation est très fréquente sur l'internet où un internaute français va, par exemple, se connecter sur le site d'une filiale d'une société américaine, laquelle enverra ensuite les données collectées à sa maison-mère. Cependant, le niveau de protection étant beaucoup plus faible aux Etats-Unis, les données ne bénéficieront pas d'une protection équivalente à celle qui est garantie par la France.

La Directive Européenne de 1995 n'autorise donc ce transfert vers des pays extérieurs à l'Union Européenne que sous conditions. Il faut que les pays destinataires des données assurent un niveau de protection suffisant ou adéquat de la vie privée et des libertés et droits fondamentaux de la personne à l'égard des traitements dont ces données font l'objet ou peuvent faire l'objet. Si le niveau de protection dans le pays vers lequel les données doivent être transférées n'est pas adéquat, le transfert est interdit.

Toutefois, une série d'exceptions permet au responsable du traitement de transférer ces données, notamment si la personne a consenti expressément à leur transfert.

5. Le droit européen s'applique-t-il lorsqu'une entreprise américaine collecte les données en Europe ?

Dans ce cas, c'est bien le droit européen tel que décliné dans les différents pays de l'Union qui s'applique.

6. Dans le cas des flux transfrontaliers de données entre l'Union Européenne et les Etats-Unis, il existe cependant une particularité.

Les principes du dispositif Safe Harbor ont été négociés entre les autorités américaines et la Commission européenne, et s'inspirent de la Directive 95/46 du 24 octobre 1995.

La Commission européenne, par une décision du 26 juillet 2000, reconnaît à ces principes un niveau de protection adéquat aux transferts de données opérés depuis l'Union Européenne. Les organisations américaines qui adhèrent aux principes « Safe Harbor », c'est-à-dire à un système par lequel elles s'engagent à assurer un certain niveau de sécurité dans le traitement et l'utilisation des données, ne doivent donc pas se soumettre aux formalités requises pour l'obtention d'une autorisation. Des sanctions sont prévues en cas de non-respect de l'engagement.

Dans la mesure où les Etats-Unis n'assurent pas un niveau de protection adéquat selon les critères européens, ces principes permettent aux entreprises américaines de contourner les obstacles constitués par la Directive européenne de 1995 pour pouvoir utiliser des fichiers de consommateurs en provenance de l'Europe.

7. Pourquoi cela vous intéresse-t-il ?

7.1 Il est de l'intérêt de tout internaute, qui navigue sur le net, participe à des forums, consulte de nombreux sites, et achète des biens et services, d'avoir une idée de la protection qui s'applique aux données personnelles qu'il fournit.

Cette protection est ainsi à géométrie variable selon le site consulté (ex : site américain adhérent ou non aux principes Safe Harbor), mais aussi selon le niveau de conscience de l'internaute des atteintes possibles à sa vie privée (ex : certains réseaux sociaux permettent à l'internaute d'afficher ses opinions politiques, etc.). Mieux informé, l'internaute peut, en effet, décider de délivrer ou non ces renseignements privés.

7.2 Le défaut d'harmonisation au niveau mondial des règles de protection des données personnelles demeure, même si aujourd'hui le nombre de pays ayant opté pour l'élaboration d'une législation protectrice a augmenté.