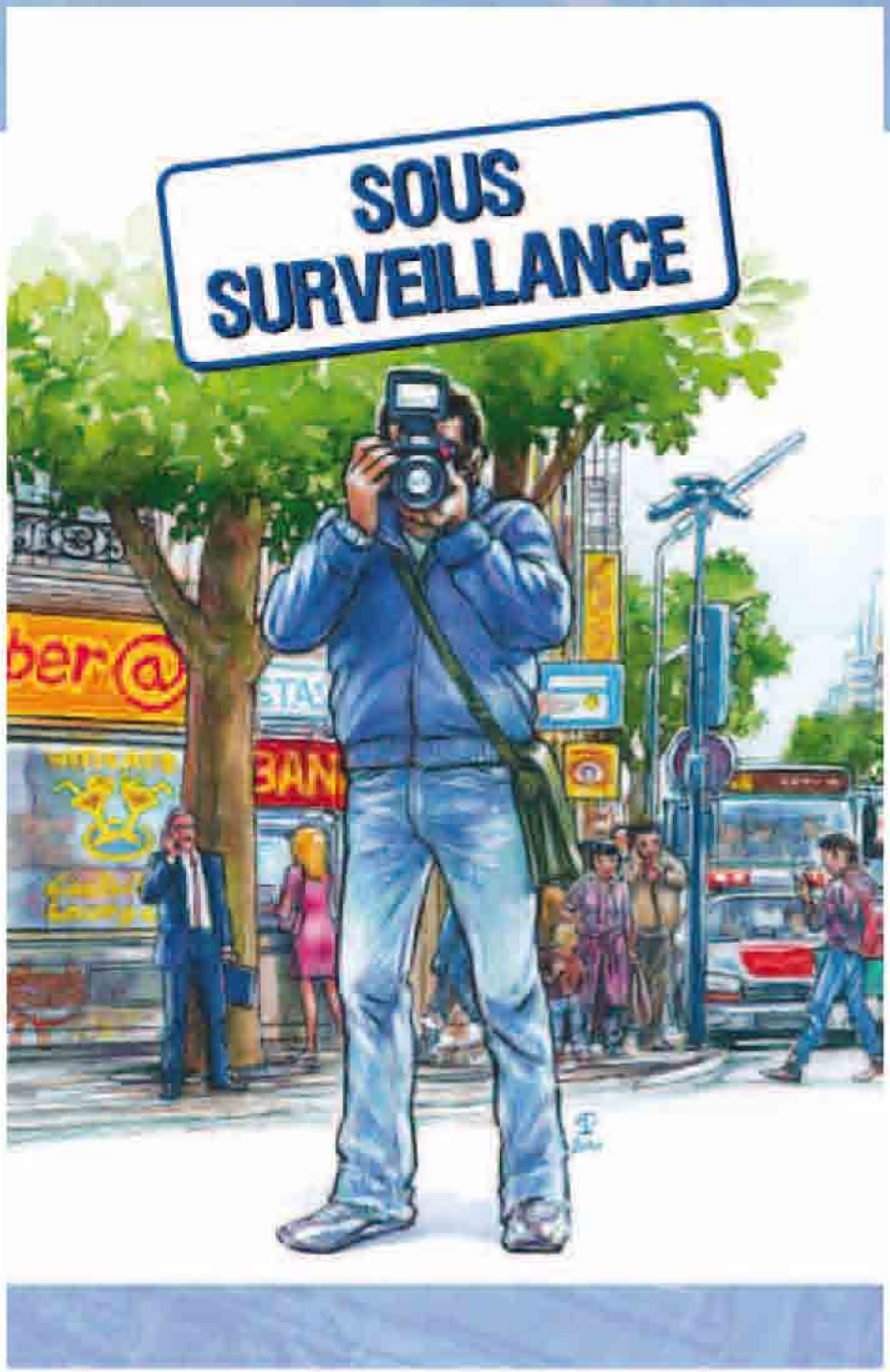
DOSSIER DE PRESENTATION

DONNEES PERSONNELLES, DES DROITS ?



Contact : service communication LDH
Anne Garacoïts : 01 56 55 51 08
anne.garacoits@ldh-france.org
www.ldh-france.org

Ligue des droits de l'Homme

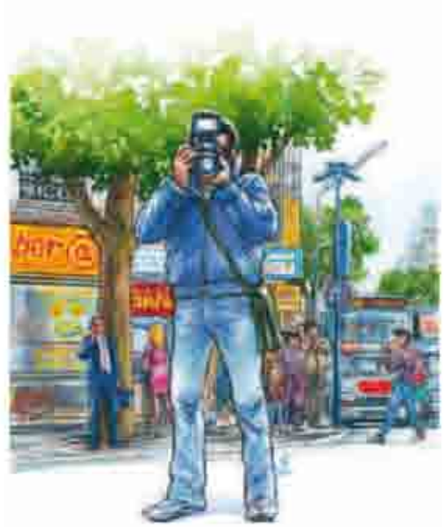
SOMMAIRE DU DOSSIER

LA BANDE DESSINEE « SOUS SURVEILLANCE »

SOUS SURVEILLANCE :

Dans une ville européenne indéterminée, des jeunes travaillent, étudient, voyagent, tiennent des blogs, publient sur des forums, se retrouvent au concert... Un épisode très « délicat » de la vie d'un jeune photoreporter, la mobilisation de ses amis pour le sortir de cette situation illustrent les atteintes à la protection des données personnelles que peut induire l'utilisation des nouvelles technologies. La BD en souligne les conséquences mais aussi les recours possibles.

Un glossaire et une information sur des sites utiles complètent cette BD. Cet outil permettra de faire prendre conscience à notre public cible, les jeunes de 15 à 30 ans, gros « consommateurs» de Tic, des risques, de leur indiquer les moyens de se protéger et les recours en cas d'abus.



A partir du 22 avril 2010, vous pourrez consulter la BD dans sa version flipbook sur www.ldh-france.org

Un outil pour sensibiliser les jeunes à la protection des données personnelles :

« Sous surveillance » est déjà diffusée via le réseau de sections, fédérations et régions de la LDH à travers des rencontres, débats, forums...etc. Cet outil a vocation à servir de support de sensibilisation présenté par des professionnels, via des structures susceptibles d'accueillir des jeunes adultes, et mis à disposition pour consultation et ainsi toucher le plus largement les jeunes de 15 à 30 ans.

Ainsi, toute organisation intéressée par ce projet peut disposer de la BD pour en permettre la consultation et organiser des rencontres sur le thème de la protection des données personnelles.

La mise en ligne de la BD sur le site de la LDH permettra de toucher un plus grand nombre de personnes mais aussi d'organiser des « rencontres autour d'un écran ». Enfin, une affiche est disponible au niveau national, pour information dans les points d'accueil et incitation à la consultation en ligne, mais aussi pour les événements que vous organiserez.

Nous espérons que cet outil vous permettra éventuellement d'en savoir plus sur la protection des données personnelles, et surtout de sensibiliser notre public cible sur ces enjeux. Nous restons à votre disposition pour toute demande d'intervention, de contacts, d'organisation de débats.

EN PRATIQUE !

▶ Cette BD est gratuite (elle ne peut en aucun cas être vendue).

▶ Pour commander vos BD, merci d'envoyer un mail décrivant en quelques lignes votre projet et la quantité souhaitée à :

Anne Garacoits - service communication LDH
anne.garacoits@ldh-france.org - 01 56 55 51 08

DONNEES PERSONNELLES, DES DROITS ?

SENSIBILISER ET INFORMER LES JEUNES CITOYENS EUROPEENS

Projet coordonné par la Ligue des droits de l'Homme réalisé avec l'AEDH, EDRi, IuRe, Pangea.
Financé par la Direction générale justice liberté sécurité de l'Union européenne.
Programme «Droits fondamentaux et citoyenneté» (2007-2013)

ELABORATION ET OBJECTIFS DU PROJET « DONNÉES PERSONNELLES, DES DROITS »

En répondant à l'appel à proposition de la Direction générale justice liberté sécurité de l'Union européenne la LDH et ses partenaires avaient pour objectif de sensibiliser et informer les jeunes adultes sur la question de la protection des données personnelles.

Les jeunes et les jeunes adultes sont très utilisateurs de nouvelles technologies qui leur facilitent la vie courante. Le fait d'avoir à communiquer des données personnelles ne leur pose la plupart du temps aucun problème.

L'Union européenne a mis en place un ensemble législatif et réglementaire qui vise à assurer aux citoyens la protection de leurs données personnelles comme étant un des droits fondamentaux. Le Traité de l'Union européenne fait référence à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales qui prévoit que **« toute personne a le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».**

Le traité de Lisbonne consacre la valeur juridique de la Charte des droits fondamentaux. Ainsi **« toute personne a le droit à la protection des données personnelles la concernant »**. Ces données ne peuvent être traitées sans le **« consentement de la personne concernée »**, et celle-ci a le droit d'accéder aux données collectées. Il doit y avoir soumission du respect de ces règles de droit à une autorité indépendante.

Le projet s'inscrit dans l'objectif général de « la promotion du développement d'une société européenne fondée sur le respect des droits fondamentaux » avec l'objectif spécifique de « promouvoir les droits fondamentaux et informer les personnes de leurs droits » :

- Aider les jeunes et les jeunes adultes à prendre conscience de la question sensible de la protection des données personnelles, auxquelles ils ne prêtent habituellement pas attention, alors qu'elles peuvent être collectées et traitées à leur insu lors de démarches semblant anodines. Nous abordons là un des thèmes de la Charte des droits fondamentaux, dont l'importance croit avec la diversification de l'utilisation des nouvelles technologies de l'information et de la communication (NTIC).
- Aborder cette question d'un point de vue européen, avec l'idée de mettre en place des outils transposables dans tous les pays, et dont la conception est basée sur les difficultés et les lacunes enregistrées dans plusieurs pays.

Nous avons donc travaillé sur deux volets, avec quatre partenaires : deux réseaux européens, l'AEDH et EDRI, une association tchèque (IuRe), une association espagnole (Pangea):

- **une analyse des technologies, de la législation qui les régit, et des risques liés à leur utilisation avec des recommandations ;**
- **la production d'un outil de sensibilisation, la BD** *Sous surveillance.*

PRESENTATION

TECHNOLOGIES, LEGISLATION, RISQUES

Quatre thèmes d'utilisation des technologies de l'information et de la communication (Tic) mettant en cause la protection des données personnelles ont été retenus et étudiés dans neuf pays dont la France selon une grille commune d'analyse :

- **Mobilité et transports** (cartes de transport, PNR, géo-localisation)
- **Identité biologique** (passeport biométrique, contrôles d'accès : entreprises, établissements scolaires)
- **Communications interpersonnelles** (messageries, téléphone)
- **Réseaux sociaux** (internationaux ou locaux)

Contexte historique

Il y a en France une longue tradition de combats pour les droits et libertés. Ainsi, la Déclaration des droits de l'Homme et du citoyen, issue de la révolution de 1789, est intégrée dans le préambule de la Constitution.

C'est en 1976 que le Parlement est saisi d'un projet destiné à protéger par une loi et une nouvelle institution les libertés et droits fondamentaux, dont la vie privée, à l'égard des fichiers et traitement de données personnelles. La Commission nationale informatique et libertés (la Cnil, première autorité indépendante instituée en France) sera créée par la loi du 6 janvier 1978 dite loi « Informatique et libertés ». Elle est l'aboutissement d'un combat initié en 1974 avec la révélation reprise par toute la presse, de l'informatisation d'un fichier centralisé dénommé Safari (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à affecter un numéro unique à tout Français dès sa naissance. Ce numéro unique devait faciliter les interconnexions de fichiers et les échanges d'information entre administrations. Cette mobilisation sera l'occasion également de révéler à l'opinion l'existence de fichiers de police occultes et la mise en place de techniques de profilage pour détecter les enfants « à risques » (médicaux ou sociaux) à partir du fichier Gamin (Gestion automatique de la médecine infantile), qui répertoriait les résultats des examens de prévention médicale passés par tous les enfants à trois, six et dix-huit mois.

L'idée d'un identifiant unique, qui avait été imaginé pendant la Seconde Guerre mondiale sous le régime de Vichy, et mis en place depuis 1946 dans une version édulcorée (suppression des codes « femme ou homme juif ») pour gérer la sécurité sociale des personnes salariées, devait acquérir avec Safari une dimension et puissance nouvelle au moment où l'informatique envahissant les grandes organisations, ré-ouvrait la porte sur le long terme à toutes les craintes du totalitarisme selon des images «orwelliennes ».

Législation en vigueur

Informatique, fichiers et libertés :

Conçue sur des principes généraux, universels et intemporels, la loi du 6 janvier 1978 a fait l'objet d'une dizaine de modifications destinées à en préciser l'application dans certains domaines (recherche médicale par exemple).

Les deux premiers articles de la loi posent le cadre de la protection des données personnelles et définissent les notions de données personnelles et des traitements concernés :

> « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* »

> *« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »*
>
> *« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »*

Les articles 6 et 7 définissent les principes s'appliquant aux données personnelles :

- **Le principe de pertinence et de proportionnalité des données :** les données doivent être adéquates, pertinentes et non excessives par rapport à la finalité du traitement.
- **Le principe d'une durée de conservation limitée :** les données ne doivent être conservées que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées.
- **L'obligation de ne communiquer les données qu'aux destinataires et aux tiers autorisés.**
- **L'obligation de sécurité :** tout responsable de traitement de données doit prendre toutes précautions utiles afin de préserver la sécurité des informations
- **Le principe de loyauté et de transparence :** toute personne doit être informée des conditions d'utilisation de ses données. Elle a un droit d'accès à ses informations, de les faire rectifier voire supprimer et, sous certaines conditions, de s'opposer au traitement de ses données.
- **Les interconnexions doivent faire l'objet d'une autorisation :** elles constituent un nouveau traitement et justifient l'application du principe de finalité.
- **Le principe de finalité** : un traitement ne peut être mis en œuvre que pour une finalité déterminée, explicite et légitime.

L'article 8 prohibe la collecte et le traitement de données à caractère personnel qui font apparaître « *les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicales des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* .»

LE SECRET DES CORRESPONDANCES émises par la voie des communications électroniques est garanti par la loi (loi du 10 juillet 1991, extension du principe général du secret des correspondances). *« Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.* »

LA CONFIANCE DANS L'ÉCONOMIE NUMÉRIQUE (LCEN 21 juin 2004) : La transposition de la directive européenne du 8 juin 2000 établit un droit français de l'internet et pose les règles relatives au commerce électronique. La LCEN définit les communications sur l'internet en créant de nouvelles catégories légales et établit un régime de responsabilité pour ses acteurs.

PASSEPORT BIOMÉTRIQUE : Il a été institué par de simples décrets (30 décembre 2005 et 30 avril 2008) qui ont été attaqués par la LDH devant le Conseil d'Etat pour violation du principe de proportionnalité. Alors que ces passeports sont délivrés depuis juin 2009, l'examen de la requête est toujours en cours.

PNR : Le ministre de l'Intérieur est autorisé à créer des traitements automatisés des données à caractère personnel (PNR et APIs) recueillies à l'occasion des déplacements internationaux (Art.7 de la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme). Quant aux douanes, c'est l'art.65 du Code des douanes qui leur permet de requérir ponctuellement les données PNR de certains vols. Le Sénat s'est prononcé sur l'utilisation des PNR à des fins répressives (E 3697). Il a énoncé un grand nombre de réserves et préconisé un grand nombre de dispositions de protections (résolution n° 84 du 30 mai 2009).

Evolution de la législation

Au motif d'offrir plus de sécurité, la tendance est à l'utilisation de plus en plus poussée des Tic pour la surveillance des citoyens dans tous les domaines de la vie. Cette tendance conduit à une surveillance et une suspicion généralisée.

Protection des auteurs du téléchargement illégal

(LOI « RÉACTION ET INTERNET » DITE « HADOPI » : HAUTE AUTORITÉ POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES DROITS SUR INTERNET)

La loi prévoyait que œle repérage des « pirates » se ferait par des sociétés privées, les ayants droit et producteurs d'œuvres, qui signaleraient à la Hadopi (première autorité administrative indépendante créée pour restreindre les droits et libertés) les adresses IP des présumés « pirates ». Cette autorité devait pouvoir prononcer des sanctions (coupure d'accès Internet, amendes…). En juin 2009 le Conseil constitutionnel a demandé que ce soit un juge qui prononce cette sanction.

La nouvelle loi votée en septembre 2009 confie au juge des référés le pouvoir de prononcer une suspension de l'accès internet pour une durée d'un an maximum, aux agents de l'Hadopi le pouvoir de constater les infractions. A l'objection que l'abonné n'est pas forcement le coupable de l'infraction (accès wifi non sécurisés, etc.) le législateur a répondu par la création d'une contravention sanctionnant la « négligence caractérisée » du titulaire d'un abonnement qui laisse commettre des téléchargements illégaux sur son ordinateur…
Outre les nombreux problèmes techniques et les exigences contradictoires vis-à-vis des fournisseurs d'accès à Internet (FAI) que pose cette loi, elle pose le problème de « proportionnalité entre l'atteinte à la vie privée (collecte des adresses IP et coupure de l'accès Internet), et le respect du droit de propriété » (protection des auteurs). En outre, la procédure judiciaire prévue n'assure pas nécessairement les droits de la défense.
Pour limiter le nombre de téléchargements illégaux, sauvegarder les intérêts de quelques entreprises, les autorités publiques instaurent un système de suspicion généralisée et compromettent le droit au respect de la vie privée. Cette loi, même si elle est jugée inapplicable, met en péril les libertés et les droits fondamentaux des citoyens. **On peut ainsi s'inquiéter de ce qu'un tel dispositif, que certains autres Etats européens ont annoncé vouloir également mettre en œuvre (Grande Bretagne notamment), pourrait être utilisé à d'autres fins que la protection de la création sur Internet.**

Sécurité intérieure

(LOPPSI - 2 : LOI D'ORIENTATION ET DE PROGRAMMATION POUR LA PERFORMANCE DE LA SÉCURITÉ INTÉRIEURE)

En cours de discussion en début 2010, cette loi renforce encore la surveillance des citoyens. Elle prévoit notamment que les services de l'Etat pourront utiliser des mouchards, sans le consentement des intéressés, pour accéder aux données informatiques, les collecter, les enregistrer, les conserver et les transmettre, sans que la légalité des ces mouchards ne soit vérifiée.

La création d'un fichier nommé Pericles permettra de rapprocher tous les fichiers judiciaires, de croiser tous les renseignements disponibles pour lutter contre tous les types de délinquance et notamment la pédopornographie.

La LDH a tenu à alerter les élus sur la dangerosité de ce projet (11 février 2010) : «*Le projet de loi Loppsi, est porteur d'un saut qualitatif considérable dans la construction d'une société de la surveillance, du soupçon et de la peur. Même s'il se présente comme un fourre-tout hétéroclite, sa logique est claire : il s'agit de renforcer, d'intégrer et de concentrer tous les instruments disponibles de fichage, de traçage et de contrôle social dont les gouvernants actuels sont sans cesse plus demandeurs. »*

Les Autorités de protection des données personnelles

La Commission nationale informatique et libertés (Cnil)

« L'INFORMATIQUE DOIT RESPECTER L'IDENTITÉ HUMAINE, LES DROITS DE L' HOMME, LA VIE PRIVÉE ET LES LIBERTÉS »

La Cnil a été créée par la loi « Informatique et libertés » en 1978. Elle est composée de dix-huit commissaires, nommés pour cinq ans. Ces commissaires sont des élus nationaux des deux chambres (4), des hauts magistrats (6), des représentants du Conseil économique et social (2) et des personnalités qualifiées (5) désignés par les présidents de l'Assemblée nationale et du Sénat et par le gouvernement. Son actuel président est sénateur. 120 agents assurent les missions quotidiennes de la Cnil ce qui est tout à fait insuffisant au regard de la charge qui lui incombe.

Pour atteindre les objectifs prévus par la loi, prévenir les dangers que l'informatique peut faire peser sur les libertés, protéger la vie privée et les libertés individuelles ou publiques et sanctionner les abus, la Cnil dispose de différents pouvoirs : décision, contrôle, sanction, recommandation.

En 1978 ces pouvoirs s'exercent dans six principales missions[1] :

- **accorder ou refuser les autorisations préalables** à la création de fichiers de traitement de données personnelles ;
- **informer** les personnes de leurs droits et obligations en matière de protections relatives à la vie privée, de la liste des fichiers existants et des traitements pour lesquels ils sont déclarés ;
- **garantir** le droit d'accès, pour le compte des personnes qui en font la demande, aux fichiers de police et de la défense ;
- **contrôler** la sécurité des systèmes d'information concernant les traitements des données : exactitudes des contenus, communication à des personnes non autorisées, etc. La Cnil fait procéder aux modifications nécessaires, tels que la rectification ou l'effacement de données inexactes ;
- **sanctionner** les responsables des fichiers qui ne respectent pas la loi, en adressant un avertissement, une mise en demeure, des sanctions pécuniaires, une injonction de cesser le traitement, voire même une dénonciation au Parquet des contrevenants.
- **réglementer.** La Cnil établit des normes simplifiées afin que les traitements les plus courants et les moins dangereux pour les libertés fassent l'objet de formalités allégées.

Il faut souligner que la dernière modification, en août 2004, sous couvert d'une mise en conformité avec la directive européenne du 24 octobre 1995, a considérablement amoindri le régime d'autorisation préalable qui donnait jusqu'alors à la Cnil la compétence générale pour refuser la mise en œuvre de fichiers dans tout le secteur public. L'autorisation préalable est supprimée notamment dans le domaine le plus sensible pour les libertés, celui de la constitution de fichiers de police et celui de l'identité biométrique administrative éventuelle, retirant ainsi une large efficacité à la Cnil. La création de la profession de « correspondants informatique et libertés» dans les entreprises permet à celles qui nomment un salarié à cette fonction de se dispenser de déclaration à la Cnil pour la mise en œuvre de traitements automatisés de données personnelles. Les demandes d'autorisation sont cependant maintenues. Par contre, la nouvelle loi a renforcé les pouvoirs de la Cnil en matière de contrôle préalable dans des domaines sensibles relevant du secteur privé et lui a conféré un pouvoir de sanction.

Dans son rapport de 2008 le président de la Cnil remarque : *« Plus aucun secteur d'activité, plus aucune parcelle de notre vie individuelle et collective, n'échappe désormais au développement et à la pression des technologies »*. Mais bien que 12 emplois aient été créés, la Cnil manque de moyens pour traiter les problèmes posés, en 2008, 3 500 demandes n'ont pas pu être traitées !

Les associations de défense des droits et libertés demandent le renforcement du caractère pluraliste et démocratique de la Cnil. Lors de son congrès en 2009, la LDH demandait notamment à propos de la surveillance des citoyens : *« (…) des contrôles d'Autorités réellement «indépendantes» par leur composition, dont les décisions doivent être portées à la connaissance des citoyens et qui doivent disposer de pouvoirs juridiques réels (pouvoir d'autorisation des fichiers d'Etat, pouvoirs d'intervention et de contrôle sur la gestion des fichiers de police et de gendarmerie) et de moyens à la hauteur de leurs tâches… »*

1 Informations recueillies à partir du site http://wiki.univ-paris5.fr/wiki/CNIL

La Commission nationale de contrôle des interceptions de sécurité (CNCIS)

C'est l'autorité de protection des données personnelles chargée de veiller au respect des dispositions du **titre II « Des interceptions de sécurité »** de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, modifiée notamment par la loi du 23 janvier 2006. La Commission nationale est chargée du contrôle des demandes de communication des données prévues par l'article L. 34-1-1 du Code des postes et des communications électroniques.

La sensibilisation aux questions de vie privée

Depuis plus de trente ans, en France, les droits et libertés des citoyens au regard de l'informatique et des technologies de l'information et de la communication sont en principe protégés par de nombreux dispositifs renforçant ceux mis en place au niveau de l'UE. Pour autant, ces dispositifs se révèlent insuffisants dans un monde globalisé où les volontés politiques sont dirigées vers une plus grande surveillance du citoyen sous le prétexte d'assurer la sécurité, de lutter contre le terrorisme. Les intérêts industriels et commerciaux exploitent les décisions politiques à leur profit, les avancées technologiques influençant les besoins (biométrie, RFID, vidéosurveillance…).

Au fil des projets gouvernementaux, les mobilisations ont été nombreuses pour combattre le fichier Stic, la carte d'identité infalsifiable « Identité nationale électronique sécurisée » (Ines), le passeport biométrique, le fichier Eloi, les fichiers Sconet et Base-élèves premier degré, les fichiers Edvige, Cristina, le Fnaeg, la vidéosurveillance, les deux nouveaux fichiers remplaçant Edvige, etc.

Des mobilisations à l'efficacité inégale

Parmi les nombreuses campagnes menées contre les atteintes à la vie privée et aux libertés on peut citer :

Edvige (Exploitation documentaire et valorisation de l'information générale)

A l'été 2008, une très forte mobilisation a eu lieu (700 organisations et 250 000 personnes) contre la mise en place, par décret gouvernemental, d'un fichier dénommé Edvige susceptible de porter atteinte à la vie privée et aux libertés. Le Conseil d'Etat a censuré une partie du décret, obligeant le gouvernement à revenir en partie sur la finalité et le contenu du fichier.

Vidéosurveillance publicitaire

A la fin de l'année 2008, la RATP a annoncé l'installation dans les couloirs du métro de 400 écrans publicitaires dits « intelligents », équipés de caméras techniquement capables de « *déterminer le sexe des passants, leur âge, la couleur de leur peau, le type de vêtements portés* », et d'analyser « l'*expression faciale* » toute en précisant la « *zone de l'image regardée* ». La mobilisation des associations, notamment Résistance à l'agression publicitaire (Rap), a obligé la RATP à renoncer au mois de juillet 2009.

Le fichier Eloi (arrêté du 18 août 2006)

Il est contesté par plusieurs associations devant le Conseil d'Etat. Celui-ci l'a annulé estimant qu'un tel outil devait donner lieu à un décret et passer par la Cnil. Par décret du 26 décembre 2007 une seconde version du fichier Eloi apparaît (version expurgée de l'arrêté de 2006), cependant des points soulevés dans le premier recours demeuraient. Une nouvelle requête en annulation a été déposée par les associations devant le Conseil d'Etat. Deux mesures ont été annulées le 30 décembre 2009 : l'enregistrement du numéro AGDREF dans les données relatives à la personne d'origine étrangère faisant l'objet de la mesure d'éloignement, la durée de conservation de trois ans des données à compter de la date de l'éloignement effectif, lorsque la procédure a pu être mise en œuvre.

Base-élèves

L'application informatique « Base-élèves premier degré » permet la gestion administrative et pédagogique des élèves de la maternelle au CM2 dans les écoles publiques ou privées. La Base-élèves, expérimentée depuis 2005 en lien avec la Cnil, est en cours de généralisation en 2009. Les renseignements fournis par ce fichier étaient au départ considérables (culture d'origine, nationalité, date d'arrivée sur le territoire, la langue parlée à la maison, parcours et des indications aussi personnelles que la façon dont l'enfant se rend à l'école, …).

Des directeurs ont refusé d'enregistrer ces données, s'inquiétant des accès aux fichiers, transmises notamment aux maires des communes, aux inspecteurs d'académie et du manque de sécurité de cet accès. Des plaintes ont été déposées par des parents et la mobilisation s'est amplifiée. Elle a porté ses fruits puisque le ministère est revenu sur le contenu.

Ce fichage des enfants a paru suffisamment dangereux au Comité des droits de l'enfant de l'Onu pour qu'il indique fin 2009 au gouvernement français sa préoccupation quant à « l'insuffisance de dispositions légales propres à prévenir son interconnexion avec les bases de données d'autres administrations ». Il s'est notamment dit préoccupé par « l'insuffisance de dispositions légales propres à prévenir son interconnexion avec les bases de données d'autres administrations ».

Si quelques victoires ont été obtenues, il faut bien constater qu'une petite minorité de citoyens s'est mobilisée dans ces combats qui restent le fait de militants attentifs. La Cnil estime qu'à peine un tiers des Français sont conscients des problèmes de libertés individuelles posés par le développement des technologies de fichage. **Les jeunes font massivement partie des deux tiers de personnes peu ou pas conscientes des risques liés aux Tic.**

La protection de la vie privée : les services, le commerce et la valeur marchande des données personnelles

Les nouveaux enjeux de la protection de la vie privée ne sont plus seulement du coté des administrations et de leurs fichiers (même si le contrôle des citoyens par l'Etat est toujours plus intrusif), ils sont aussi du coté des entreprises privées. Non seulement chaque individu est fiché sciemment comme salarié, chômeur, contribuable, assuré social, abonné au téléphone, à Internet, mais aussi comme client d'au moins une chaîne de magasins, titulaire d'un compte en banque, client « privilégié » SNCF ou autre... Les risques et les inquiétudes en matière de vie privée, avec la multiplication des données qui circulent de façon beaucoup plus fluide, se déplacent des « grands fichiers » vers les « traces » et des administrations vers les opérateurs privés.

Les nouvelles formes de collecte et de traçage (internet, biométrie), la dimension internationale de la collecte (sites internet) et des transferts de données (division internationale du travail par le recours de plus en plus massif à la sous-traitance dans des pays hors d'Europe), la valeur marchande attribuée aux données personnelles, la puissance des moteurs de recherche permettant d'opérer des croisements, ont considérablement changé la nature des risques et leur perception. S'ajoutent à ces collectes de données personnelles par des entreprises, les flux de celles qui sont délivrées sur les réseaux sociaux.

Néanmoins les campagnes de protestations contre l'utilisation indue, la vente des données par des fournisseurs de services, des opérateurs, sont à peu près inexistantes. Seuls quelques juristes, quelques experts tentent d'alerter les individus.

On se heurte ici au fait que les technologies offertes rendent la vie plus facile, les contacts virtuels plus nombreux et que le prix à payer (délivrer ses données personnelles une seule fois) semble dérisoire aux individus mal informés. L'idée de « n'avoir rien à se reprocher » les incite à ne rien cacher.

Les risques

Mobilité et transports : traçage

Les utilisateurs des passes Navigo n'ont que très peu conscience qu'ils sont susceptibles de « disséminer », avec la puce RFID de leur titre de transport, leurs données personnelles. La géo-localisation induit un très fort risque de traçage.

L'identité biologique : identité déclarative, identité physique

L'utilisation de données biométriques dans le passeport biométrique pose le problème de l'utilisation de cette technologie à des fins d'identification par le corps. La biométrie change radicalement la nature des rapports sociaux en substituant une identité purement physique à une identité déclarée. L'utilisation de la biométrie par les enfants pose en plus le problème de l'accoutumance recherchée par les pouvoirs publics à ce type de contrôle.

Communications interpersonnelles : piratage et utilisation marketing

L'utilisation de la messagerie électronique pose le problème de la non protection des coordonnées de l'abonné, de leur vente, de leur utilisation par des sociétés de marketing. Elles peuvent par ailleurs être piratées avec risque d'usurpation d'identité. Gérée par un fournisseur d'accès à Internet (FAI), la messagerie fait l'objet de rétention des données de connexion et de certains éléments des courriels dans le cadre de la lutte contre le terrorisme. A noter que ce risque de géo-localisation à l'insu de l'abonné se retrouve avec l'utilisation des téléphones portables.

Réseaux sociaux : paramétrage, récupération et effacement des données

Les atteintes à la vie privée résultent le plus souvent d'un manque de connaissance des paramétrages qui permettent de protéger ses données personnelles en ne rendant publiques que certaines informations publiées. Les révélations très médiatisées de problèmes advenus à certains utilisateurs de réseaux sociaux ou blogueurs ont sensibilisé quelques adeptes qui réclament un droit de récupération et d'effacement de leurs données. Les SNS américains refusent de considérer le droit européen comme s'appliquant à leurs activités en Europe.

Conclusion et recommandations

Cette étude sur les pratiques d'un public « jeunes – jeunes adultes » nous a montré qu'il n'est pas facile d'obtenir des informations sur cette cible hormis les utilisations de la téléphonie et des réseaux sociaux. Néanmoins ce travail nous amène à conclure que les pratiques à l'égard de la protection des données personnelles sont généralement laxistes, peuvent porter atteinte à la vie privée et être potentiellement dangereuses.

Elles rendent nécessaire un travail d'information et de sensibilisation :

- Auprès des « usagers » ou utilisateurs des :
  - transports ou autres accès avec cartes à puce RFID ;
  - passeports et autres moyens d'identification par la biométrie ;
  - outils de géo-localisation ;
  - messageries internet et téléphones portables ;
  - réseaux sociaux.
- Auprès des pouvoirs publics français concernant :
  - la multiplication des lois et règlementations visant la surveillance des citoyens dans le cadre de
  - la lutte contre le terrorisme et le crime organisé, pour une sécurité accrue ;
  - la mise en place de ces dispositifs et l'inflation d'outils favorisant le marché industriel des technologies de surveillance au détriment de l'humain ;
  - de la multiplication d'interconnexions de fichiers.
- Auprès des instances décisionnelles de l'Union européenne et notamment en utilisant les pouvoirs conférés au Parlement depuis l'entrée en vigueur du Traité de Lisbonne :
  - pour le respect des textes fondamentaux protecteurs de la vie privée notamment dans tous les accords avec des pays tiers et les mesures de lutte contre le terrorisme et l'immigration ;
  - pour que l'Union installe une Autorité de protection des données personnelles dotée de réels pouvoirs ;
  - qu'elles fassent respecter par le droit européen les sociétés américaines.

Le travail à initier ou poursuivre comporte deux volets : les revendications à porter auprès des pouvoirs publics et des décideurs et les campagnes d'information et de sensibilisation.

Les demandes auprès des pouvoirs publics français :

- respecter et faire respecter tous les principes de la loi « Informatique et libertés » (énoncés au § « Législation ») notamment en ce qui concerne les passeports biométriques et leurs bases de données mais aussi dans les données recueillies dans différents domaines (passe Navigo, messageries, fournisseurs d'accès Internet) ;
- redonner à la Cnil tous ses pouvoirs et notamment ceux qui lui ont été retirés en 2004 et les moyens d'une indépendance réelle en revoyant le mode de désignation de ses membres pour en assurer l'indépendance politique ;
- limiter le nombre d'agents de l'Etat ayant accès aux bases de données et donner des informations et des garanties sur le strict encadrement de ces accès ;
- interdire la cession à des organismes privés des données recueillies par un organisme public ;
- afficher une transparence quant à l'absence de liens entre les intérêts des industriels des technologies de surveillance et la mise en place de nouvelles législations ;
- œuvrer pour le respect des droits fondamentaux dans tous les textes législatifs et notamment dans ceux qui concernent les collectes de données personnelles ;
- donner des moyens pour des campagnes d'information des citoyens et notamment des jeunes sur leurs droits, sur les risques de l'exposition de soi sur internet et les réseaux sociaux. Des campagnes intéressantes sont initiées par la Cnil et d'autres organismes : elles mériteraient une plus grande médiatisation et d'être largement popularisées dans les établissements accueillant des jeunes de tous niveaux scolaires.

Les campagnes d'information auprès des jeunes :

Ces campagnes pourraient être initiées après des temps de réflexion prospective sur les évolutions des technologies mais aussi des mentalités. (Par exemple l'argument des risques par rapport à l'exposition sur internet dans le cadre de la recherche d'emploi renvoie parfois sur l'argument : « *d'ici 10 ans si vous n'avez pas un blog ou un profil le recruteur trouvera cela suspect…* »).

Quelques campagnes à mener :

- informations sur le passe Navigo anonyme (voir campagnes Cnil) et revendications auprès de la RATP pour que les avantages soient équivalents au Navigo classique ;
- informations sur les fonctionnalités destinées à assurer l'exercice de la liberté d'aller et venir et la protection de la vie privée en matière de géo-localisation mais aussi sur les réseaux sociaux ;
- informations sur l'utilisation abusive de la biométrie ; sur la collecte des données PNR et leur utilisation ;
- informations sur les précautions à prendre lors de la publication sur internet (messagerie, blogs ou réseaux sociaux) : vérifier les paramètres de son profil, avoir à l'esprit que les informations peuvent être visibles par plus de personnes que l'on ne croit, mais aussi peuvent impliquer des proches qui n'ont pas donné leur consentement ;
- mener des campagnes de réflexions sur les possibilités de cryptage des données, de navigation utilisant des outils d'anonymisation, d'utiliser des pseudonymes, de « brouiller le message » en publiant des informations contradictoires, des possibilités de limiter la durée de vie des informations, etc. Toutes options qui sont contraignantes et rendent l'utilisation des Tic moins fluides mais pour lesquelles l'évolution des technologies pourrait apporter une solution.

MOBILITE TRANSPORTS

Passe navigo

Titre de transport, muni d'une carte à puce, utilisé par les usagers des transports en commun d'Ile-de-France.

Selon la RATP : « *C'est une carte à puce qui vous permet de passer plus vite aux valideurs, une nouvelle technologie qui apporte modernité, fluidité, facilité à vos déplacements dans les transports en commun d'Ile-de-France.*»

Le recensement de la technologie	La technologie utilisée est celle de la *Radio frequency identification* - RFID
Technologies utilisées	RFID signifie, en français, « Identification par radio fréquence ». Cette technologie permet d'identifier un objet, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet. La technologie RFID permet la lecture des étiquettes sans contact et peut traverser de fines couches de matériaux. **Fonctionnement :** Lors de l'accès aux transports en commun l'abonné présente son passe Navigo à un lecteur qui autorise ou non l'accès (certains trajets nécessitent aussi une validation en sortie). Le lecteur-valideur lit les données de la puce RFID, sans contact : le numéro de la puce, le type d'abonnement et sa durée de validité. Le passe Navigo permet seulement de connaître la station de métro où est entré un usager et éventuellement celle où il est sorti. La durée de conservation de ces données est limitée à 48 heures (selon les exigences de la Cnil), et uniquement à des fins de détection de fraude (puce non sécurisée).
Pays d'utilisation	France
Cadre d'utilisation	Transports en commun en Ile de France
Population concernée	Potentiellement toute la population, pas de restriction d'âge et/ou de condition. Au 31 janvier 2009, Navigo comptait 4 536 000 clients (source ratp.fr) dont : 779 000 abonnements Imagine R (titre de transport destiné aux jeunes étudiants de l'Ile-de-France qui ont entre 12 et 25 ans) et 389 000 abonnements Navigo découverte. Le passe Navigo découverte, créé à la demande de la Cnil, est une version anonyme conformément au principe : « *aller et venir librement est l'une des libertés fondamentales dans nos démocraties ». Il ne contient aucune information nominative sur le voyageur* ».
% d'utilisation / âge la population concernée	Pas de statistique fiable dans le rapport utilisation / âge de l'utilisateur
Dangers connus / potentiels de cette technologie / risques	La RFID induit un risque de traçage et de profilage des personnes. Accusées de porter atteinte à la vie privée des citoyens-consommateurs et à leur liberté d'aller et venir, cette nouvelle technologie inquiète les organisations de protection des consommateurs et de défense des droits fondamentaux qui y voient un moyen de récupérer, sans son consentement, des informations sur le consommateur. Les puces non sécurisées pourraient être lues par quiconque possédant les lecteurs adéquats à l'insu des utilisateurs. Dès 2004, la Commission nationale informatique et libertés (Cnil) a placé les étiquettes à RFID parmi les technologies à risques pour les libertés individuelles, Source:http://www.cite-sciences.fr/francais/ala_cite/science_actualites/sitesactu/question_actu.php?langue=fr&sommaire=1&id_article=2803
Les fichiers générés et leur objet	Selon les conditions générales d'utilisation : les données collectées font l'objet d'un traitement automatisé dont la finalité est la gestion de l'abonnement à la carte orange et de la demande de passe Navigo. (Délibération 2008-161 du 3 juin 2008 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport public). (décision d'autorisation unique Cnil n°AU- 015) - (Jorf n°0153 du 2 juillet 2008)

Date de création	2003
Finalité du fichier	La gestion, la délivrance et l'utilisation des titres de transport, la gestion et le suivi des relations commerciales, la gestion des analyses statistiques, la mesure de la qualité du fonctionnement du système.
Contenu, types de données	- l'identité (civilité, sexe, nom, prénom) ; - la date et le lieu de naissance ; - l'adresse postale ; - les numéros de téléphone (personnel et portable) et l'adresse courriel (facultatifs) ; - la photographie d'identité.
Qui le détient ? Qui y a accès ?/ Risques	Les données sont destinées au GIE Comutitres (groupement **assurant la gestion des titres communs de transport en Ile-de-France)** à ses prestataires de services, aux entreprises de transports de l'Ile de France, aux financeurs institutionnels et au Stif.
Durée de conservation ?	L'ensemble des données clients est conservé pendant la durée de la relation contractuelle, et à l'issue de celle-ci pendant deux ans. **Les données de validation contenant des informations relatives aux déplacements des personnes, peuvent être conservées pendant 48 heures au maximum et aux seules fins de lutter contre la fraude.**
Droit de regard et de rectification ?	Les droits d'accès et de rectification définis au chapitre 5 de la loi du 6 janvier 1978 modifiée s'exercent auprès du ou des services que le responsable de traitement aura désigné.
Finalité cachée du fichier et détournements/ Risques	La Cnil estime que la conservation pendant 48 heures des caractéristiques des trajets d'une personne identifiée, au prétexte de lutter contre la fraude, est contraire aux valeurs démocratiques. Elle revendiquait par conséquent pour les usagers la possibilité de voyager anonymement, « sans qu'il en résulte un surcoût par rapport au choix d'un passe nominatif ». Le message a été en partie entendu puisque le passe Navigo découverte, disponible dans certaines stations RATP et gares SNCF, coûte 5 euros. Les services de police pourraient exiger la communication des données enregistrées.
Législation en application	Dès lors que les dispositifs RFID utilisés donnent lieu à l'identification directe ou indirecte d'une personne physique, la loi « Informatique et libertés» s'applique. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20090723 .
Risques pour les libertés	Traçage, fichage et profilage des individus.
Conformité avec le droit européen	Il n'y a pas de législation européenne particulière sur l'utilisation de la technologie RFID qui relève donc de la directive générale de 1995. Voir cependant en plus la recommandation de la Commission européenne sur la « Mise en œuvre des pratiques de protection des données personnelles dans les applications RFID » du 12 mai 2009. Comme pour la vidéosurveillance, la problématique du passe Navigo contrevient à la Déclaration universelle des droits de l'Homme qui dans son article 12 rappelle que : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, …*» et dans son article 13 « *Toute personne a le droit de circuler librement…*»
Conscience des problèmes ou des risques encourus	L'ensemble des individus concernés par les possibilités de fichage, traçage et profilage ne sont pas suffisamment informés des risques liberticides de ces systèmes. Ils n'y voient que le confort et la commodité, sans percevoir les dangers.
Campagnes à mener ? Sur quels aspects ?	Des campagnes de sensibilisation sur le développement très rapide de la technologie RFID sans que le public soit informé des dangers potentiels en termes de traçage et de profilage par l'Etat et par le secteur marchand. Communiquer auprès des utilisateurs de carte Imagine R (pas de possibilité de passe anonyme et fortes incitations marketing ciblées de la part de la RATP).
Recommandations	Les risques de traçage devraient être médiatisés et dénoncés. Les risques d'accès aux données personnelles contenues dans les puces RFID pourraient être réduits par l'utilisation de puces de haute technologie. Les gestionnaires des fichiers devraient être incités à en sécuriser les accès (prévoir des pénalités en cas d'accès par des personnes non autorisées ?)

BIOMETRIE

Contrôles d'accès aux établissements scolaires et aux entreprises

Technologie utilisée	Lecteur d'empreintes digitales ou palmaires : **- Empreintes digitales** : chaque empreinte est différente ; il n'y a qu'une chance sur 17 milliards de trouver deux empreintes comportant 17 points de similitude. L'empreinte est numérisée soit par un capteur soit par un scanner d'une empreinte encrée. **- Empreintes palmaires** : capture d'une image en 3D de la main et extraction de plusieurs dizaines de points prenant en compte la largeur, la longueur, la forme des doigts, etc.
Cadre d'utilisation	Accès aux écoles et/ou restaurants scolaires. Accès aux entreprises et/ou aux restaurants d'entreprises. Le système se développe aussi pour les bibliothèques et les transports scolaires.
Législation	Loi informatique et liberté du 6 janvier 1978 modifiée le 6 août 2004. Directive n°95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. (http://europa.eu.int/smartapi/cgi/sga.doc?smartapi!celuxplus!prod!DocNumber&lg=fr&type.doc=Directive&an.doc=95&nu.doc=46) Convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La législation française est conforme à la législation européenne.
Population concernée	Jeunes à partir de l'âge de six ans. Avant cet âge, les différentes empreintes ne sont pas fixées. Adultes salariés de certaines entreprises.
Durée de conservation	Variable suivant l'utilisation des données collectées. La durée doit être en rapport avec la finalité et est définie dans l'autorisation délivrée par la Cnil.
Fichiers générés	Liens avec les fichiers des élèves dans les établissements scolaires, avec les fichiers des salariés dans les entreprises avec les droits d'accès.
Qui détient ces données ? **Qui y a accès ?**	Accès aux cantines scolaires : après un avis défavorable en 2000, la Cnil a donné son accord pour la mise en place d'une application biométrique utilisant la technologie du contour de la main pour gérer l'accès au restaurant scolaire du collège Joliot-Curie de Carqueiranne. Accès à l'établissement scolaire : la Cnil, par un avis du 26 juin 2008, a refusé l'utilisation d'un dispositif reposant sur l'empreinte digitale pour contrôler l'accès à un établissement scolaire ainsi que la présence des élèves. La Cnil rappelle que l'empreinte digitale, a contrario du contour de la main, est une biométrie à « trace ». Ces «traces » peuvent être capturées à l'insu des personnes et être utilisées notamment pour usurper leur identité.
Droit de regard et rectification	Ces dispositifs sont soumis à autorisation préalable de la Cnil, sauf les trois dispositifs suivants qui bénéficient d'une autorisation unique : 1) Contour de la main pour assurer le contrôle d'accès au restaurant scolaire – autorisation n°AU-009. 2) Contour de la main pour le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail – autorisation N° AU-008. 3) Empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels - autorisation n° AU-007. La Cnil insiste sur l'information préalable des intéressés. Les personnes concernées, en l'espèce les parents lorsqu'il s'agit d'enfants, doivent être clairement informées des conditions d'utilisation, du caractère obligatoire ou facultatif, des destinataires des informations et des modalités d'exercice des droits d'opposition, d'accès et de rectification. S'agissant des salariés : Le 19 avril 2005, le TGI de Paris a interdit à une filiale de la SNCF d'utiliser les empreintes digitales comme système de pointage. Les juges ont affirmé que « *l'empreinte digitale constitue une donnée biométrique morphologique qui permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu* » et que « *son utilisation porte atteinte aux libertés individuelles* ». Ce jugement était fondé sur la directive européenne et sur l'article L. 120-2 du Code du travail.

Dangers	• Constitution de fichiers à l'insu des individus. • Utilisation des fichiers constitués à d'autres fins que celui initialement prévus. • Possibilité de traçabilité et de profilage. • Risque d'usurpation d'identité Le Livre bleu du Gixel[1] indique : « *La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles, il faut donc faire accepter par la population les technologies utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles.* *Plusieurs méthodes devront être développées par les pouvoirs publics et les industriels pour faire accepter la biométrie. Elles devront être accompagnées d'un effort de convivialité par une reconnaissance de la personne et par l'apport de fonctionnalités attrayantes : éducation dès l'école maternelle, les enfants utilisent cette technologie pour rentrer dans l'école, en sortir, déjeuner à la cantine, et les parents s'identifieront pour aller chercher les enfants.*» http://bigbrotherawards.eu.org/IMG/pdf/Livre_bleu.pdf
Campagnes **Communication**	Conscience des risques : • Ce système est présenté comme un confort, une commodité et un facteur d'économie : plus de perte de cartes de cantine (ou de bibliothèque). Certains chefs d'établissements se targuent du fait que les parents sont unanimement favorables, que les élèves trouvent cela « ludique ». • Des voix discordantes tentent de s'élever : en novembre 2005 des militants se sont introduits au lycée de Gif-sur-Yvette pour protester et alerter l'opinion publique contre l'installation de bornes à la cantine. Leur condamnation pour destruction d'une borne biométrique a suscité des réactions mais a dissuadé d'autres manifestations. • L'ancien directeur de la Cnil, Louis Joinet, expert indépendant des Nations unies pour les droits de l'Homme, s'insurge lorsqu'il évoque ces bornes biométriques installées dans les écoles : « Parce qu'on veut faire accepter la traçabilité à des enfants de 3 ans. Parce qu'on veut leur dire qu'il est normal que leur corps soit un instrument de contrôle, comme si c'étaient des bêtes. » • Des parents d'élèves, des syndicats (de magistrats, la FSU) condamnent ces contrôles biométriques et en dénoncent les dangers, les dysfonctionnements et les coûts et « rejettent ce système dans la mesure où il habitue l'enfant à être contrôlé à l'aide d'une partie de son corps. » (FCPE de l'Hérault). • La Cnil veut poursuivre la réflexion quant à l'utilisation de dispositifs biométriques auprès des mineurs. Elle envisage de procéder à des auditions d'associations de parents d'élèves, de chefs d'établissement et de représentants du ministère de l'Education nationale.
Recommandations	Prendre appui sur les protestations des syndicats et associations de parents d'élèves et sur les avis de la Cnil et du G29 pour : - Alerter l'ensemble de la population, les parlementaires nationaux et les institutions européennes sur les dangers d'utiliser la biométrie pour l'identification des personnes. - Dénoncer les intérêts financiers des industriels qui rejoignent les intérêts politiques de contrôle des citoyens.

1 Groupement des industries de l'interconnexion des composants et des sous ensembles électroniques

COMMUNICATIONS INTERPERSONNELLES

Messagerie Gmail

Messagerie gratuite. ex : Gmail (service « offert » par Google)

Il s'agit d'un service de messagerie gratuit proposé par Google.

Les messages reçus sur le compte Gmail peuvent être lus via un client de messagerie (grâce à sa compatibilité avec les protocoles POP3 et IMAP) ou avec un navigateur web.

De nombreuses fonctionnalités du service ne sont cependant accessibles qu'à travers le navigateur web.

Technologie utilisée/outil	Envoi/réception de messages électroniques Protocoles d'envoi des courriers électroniques utilisés : SMTP (*Simple Mail Transfer Protocol*, Protocole simple de transfert de courrier) Protocoles d'envoi/réception des courriers électroniques : Pop et Imap
Utilisation	Courrier électronique (courriel) échange de textes, fichiers joints (textes, sons, images) entre différents interlocuteurs (particuliers / particuliers, les entreprises, les administrations etc.). A partir d'ordinateurs personnels ou dans des lieux privés ou publics (établissements scolaires, universitaires, cybercafés, etc.) entreprises, à partir d'ordinateurs portables dans les lieux équipés de wifi + téléphones portables (smart phones, e-phone). Ce service est « offert » par Google depuis 2006, en « contrepartie » des publicités sont affichées en fonction de mots-clés repérés dans les messages échangés. L'ouverture d'un compte Gmail ne demande que : nom, prénom, nom choisi pour l'adresse électronique et le choix d'un mot de passe. Rien ne vient vérifier l'exactitude du nom indiqué, ce nom pouvant être un pseudonyme. Il est nécessaire de lire les conditions générales d'utilisation afin de savoir que : « **des copies résiduelles de vos messages pourront rester stockées sur nos système, même après que vous les aurez effacées de votre boîte aux lettres ou que vous aurez fermé votre compte** ».
Législation	Google adhère aux principes de la déclaration de confidentialité *US Safe Harbor* concernant la protection de la vie privée. Selon la Cnil, Google refuse pour le moment de se soumettre à la législation européenne sur la protection des données pour les raisons suivantes : • considère que la loi européenne sur la protection des données ne lui est pas applicable alors même qu'il dispose de serveurs et d'établissements en Europe ; • souhaite conserver les données personnelles des internautes relatives à l'usage du moteur de recherche au-delà des 6 mois maximum demandés par le G29 sans aucune justification ; • n'apporte aucune amélioration à ses mécanismes d'anonymisation des requêtes sur le moteur de recherche qui sont pourtant insuffisants ; • considère que les adresses IP sont des données confidentielles mais non personnelles, ce qui a pour effet d'éviter d'accorder certains droits à ses utilisateurs ; • ne manifeste pas la volonté d'améliorer et clarifier les modalités du recueil du consentement des utilisateurs.

Statistiques	Population concernée : selon ComsCore Media Metrix, en décembre 2008 Gmail comptait **3,6 millions de visiteurs uniques** (connections Gmail à l'exclusion des accès publics et téléphones). En 2009, 149 millions d'internautes utilisent ce service de messagerie électronique. Notons qu'une proportion importante de jeunes n'ayant pas d'abonnement internet avec un FAI classique ont un compte messagerie Gmail accessible à partir de n'importe quel accès internet.
Contenu du fichier **Finalité du fichier**	**Qu'est-ce qui motive selon Google l'inscription dans le fichier ?** Améliorer la qualité des services. Google utilise les cookies « ainsi que d'autres technologies » pour « […] en savoir davantage sur votre façon d'utiliser les services Google, ce qui nous permet de développer la qualité de nos services ». Les informations d'ordre personnel fournies lors de l'inscription sont stockées par Google et peuvent être regroupées avec d'autres informations fournies pour d'autres services Google ou des services tiers pour « offrir un meilleur confort d'utilisation ». Les serveurs Google enregistrent automatiquement certaines données, notamment l'URL, l'adresse IP, la langue et le type de navigateur utilisés ainsi que la date et l'heure auxquelles l'utilisateur a effectué sa requête. **Finalité du fichier :** Selon Google : « *vous rendre service !* » Google assure la maintenance et le traitement de votre compte Gmail et de son contenu afin de vous fournir le service Gmail et d'améliorer nos prestations. Les ordinateurs de Google traitent les informations contenues dans nos messages à des fins diverses notamment pour l'affichage des publicités et de liens connexes, la prévention des messages non sollicités (spams), la sauvegarde de nos messages ainsi qu'à d'autres fins liées à la fourniture du service Gmail. **Contenu du fichier :** L'avis de confidentialité Gmail précise : « *Lorsque vous utilisez Gmail, les serveurs de Google enregistrent automatiquement certaines informations (vos messages, liste de contacts et autres données relatives à votre compte) concernant votre utilisation du service.* *Google enregistre des informations telles que l'activité sur le compte (incluant l'espace de stockage utilisé, le nombre de connexions), les données affichées ou sur lesquelles vous avez cliqué (notamment les éléments d'interface, les annonces, les liens) et d'autres informations de connexion, comprenant le type de navigateur, l'adresse IP, la date et l'heure d'accès, les ID de cookies et les URL des pages visitées précédemment.* »
Durée de conservation	Sous la pression, Google qui entendait conserver les informations pendant 2 ans puis 18 mois, a réduit la conservation à 9 mois alors que le G 29 demande 6 mois.
Qui détient les données ? **Qui y a accès ?**	Les informations personnelles sont traitées par les serveurs de Google, aux Etats-Unis et dans d'autres pays. Dans certains cas, le traitement peut être opéré sur un serveur situé hors de France. Cela implique que pour Google, la législation qui s'applique est celle des Etats-Unis. Google ainsi que les tiers que Google autorise peuvent avoir accès à ces données. Dans les conditions générales de Google, indique qu'il veille à ce que les tiers à qui il confie éventuellement le traitement de vos informations personnelles respectent ses règles de confidentialité. Google traite les informations personnelles uniquement aux fins définies dans les présentes Règles de confidentialité et/ou dans les Avis de confidentialité propres à chaque service. Outre ce qui précède, les informations collectées sont utilisées aux fins suivantes : ▪ vous fournir les services proposés, notamment l'affichage de contenus et de publicités personnalisées ; ▪ réaliser des audits, des recherches et des analyses afin d'assurer la maintenance, la protection et l'amélioration de nos services ; ▪ assurer la maintenance du réseau ; ▪ protéger les droits ou la propriété de Google ou de ses utilisateurs ; ▪ développer de nouveaux services.

Qui détient les données ?

Qui y a accès ?

Concernant la sécurité des informations:

Gmail met en place un partage d'informations ainsi qu'un transfert ultérieur :

- lorsque vous envoyez un courrier électronique, Google inclut, dans le corps du message des informations telles que votre adresse électronique et le courrier lui-même.
- Google fournit uniquement aux annonceurs des informations non personnelles et globales comme par exemple le nombre de fois où vous avez cliqué sur l'une de leurs annonces. Google ne vend pas, ne loue pas et ne partage pas vos informations personnelles avec des tiers, excepté dans les situations spécifiques décrites dans les Règles de confidentialité de Google, notamment lorsque Google estime que la loi l'exige.

Google met en œuvre toutes les mesures de sécurité nécessaires pour empêcher tout accès et toute modification, divulgation ou destruction non autorisés des données. Ces mesures comprennent notamment des audits internes sur la collecte, le stockage et le traitement des données mais aussi des mesures de sécurité physiques visant à empêcher tout accès non autorisé à nos systèmes de stockage des données personnelles.

L'accès aux informations personnelles est strictement réservé aux employés, sous-traitants et agents Google ayant besoin d'y accéder dans le cadre de l'exploitation, du développement ou de l'amélioration de nos services. Ces personnes sont soumises à des obligations de confidentialité et sont susceptibles de faire l'objet de sanctions pouvant aller jusqu'au licenciement et aux poursuites judiciaires en cas de manquement à une de ces obligations.

Concernant la communication des informations personnelles à des tiers :

Google ne communique vos informations personnelles à des sociétés ou personnes tierces que dans les rares circonstances suivantes :

- Google a obtenu votre consentement. Il vous demande toujours votre autorisation avant de communiquer à des tiers toute information personnelle ou confidentielle vous concernant.
- Google transmet lesdites informations à ses filiales, sociétés affiliées ou autres sociétés ou personnes de confiance qui les traitent pour le compte de Google. Google veille à ce que ces dernières acceptent de traiter lesdites informations uniquement selon les instructions émises par Google et conformément aux présentes Règles de confidentialité et s'engagent à mettre en œuvre des mesures appropriées de sécurisation et de protection de la confidentialité des données.
- Google estime que l'accès, l'utilisation, la protection ou la divulgation desdites informations est raisonnablement nécessaire, dans toute la mesure permise ou requise par la loi, afin de se conformer à une obligation légale, réglementaire, judiciaire ou toute autre demande émanant d'une autorité publique, faire appliquer les Conditions d'utilisation en vigueur y compris pour constater d'éventuelles violations de celles-ci, déceler, prévenir ou traiter des activités frauduleuses, les atteintes à la sécurité ou tout problème d'ordre technique ou de se prémunir contre toute atteinte aux droits, aux biens ou à la sécurité de Google, de ses utilisateurs ou du public.

Dans le cas où Google prendrait part à une opération de fusion, d'acquisition ou à toute autre forme de cession de l'ensemble ou d'une partie de ses actifs, Google s'engage à garantir la confidentialité de vos informations personnelles concernées par les opérations mentionnées et à vous informer avant que celles-ci ne soient transférées ou soumises à de nouvelles règles de confidentialité.

Droit de regard et rectification

Les utilisateurs de Gmail peuvent modifier les données fournies lors de la création du compte.
Extrait de la « Présentation de la notion de confidentialité chez Google » :

« Nous essayons, en toute bonne foi, dans la mesure du possible et à votre demande, de vous donner accès à vos informations personnelles, de les corriger en cas d'inexactitude ou de les supprimer ».

Possibilité de supprimer son compte, l'effet est immédiat, les « copies résiduelles des messages et comptes » sont supprimées des serveurs actifs après 60 jours et « pourront être conservées sur nos systèmes de sauvegarde hors ligne ».

Dangers

- Sollicitations marketing
- Spams
- Phishing = « hameçonnage » ou « filoutage »
- Piratage des données :
  En 2008, un chercheur a démontré qu'il pouvait intercepter le contenu d'une session avec une application web, par exemple Gmail : il pouvait lire ou écrire des courriels, effacer ou modifier le carnet d'adresses ou encore changer le mot de passe de l'utilisateur légitime.
  En juin 2009, 38 experts internationaux ont écrit au dirigeant de Google pour lui rappeler les failles de sécurité de Gmail (+*Docs ou Calendar autres services gratuits de Google*) et lui demander d'y remédier.

Le système de connexion sécurisée (« https » affiché dans la barre de navigation) n'est actif que pour la saisie des identifiants (paramétrage par défaut), ensuite la connexion n'est plus sécurisée. L'option d'activation n'est pas signalée aux utilisateurs, elle reste peu accessible (dernière de 13 options de paramétrages). L'argument avancé par Google est le ralentissement du fonctionnement de la messagerie. Possible conséquence de ce piratage :

- **Usurpation d'identité**

Conscience des risques et communication

Statistiques concernant les messageries en général:

Selon un rapport du Sénat, un sondage Eurobaromètre réalisé sur un échantillon de **jeunes gens âgés de 15 à 24 ans** montre que **33 %** seulement d'entre eux ont conscience de leurs droits en matière de données à caractère personnel ; **18 %** connaissent l'existence des autorités nationales de contrôle de la protection des données.

Pourtant **20%** des jeunes seulement jugent sûre la transmission des données à caractère personnel par Internet. Malgré cette méfiance motivée par le manque d'information, les jeunes sont aujourd'hui les utilisateurs les plus familiers d'Internet et des nouvelles technologies.

Les bonnes pratiques :

- puisque rien n'y oblige ne pas déclarer sa véritable identité lors de l'ouverture d'un compte Gmail ;
- utiliser un anti-virus et un anti-spam ;
- ne pas transmettre ses données personnelles (e-mail, adresse physique du domicile, n° de téléphone, adresse de famille etc.) à l'inscription. Ne pas publier son adresse électronique sur Internet (si c'est indispensable, utiliser des astuces comme écrire « arobase » à la place du symbole @, elle ne sera pas reconnue par un robot) ;
- utiliser une adresse électronique spécifique pour les services en ligne sur Internet et une autre pour les échanges avec famille, amis et autres ;
- changer l'adresse électronique (spécifique) si elle reçoit trop de spams ;
- ne jamais répondre aux spams y compris pour protester, ceci révèlerait la validité de l'adresse ;
- lire les conditions générales d'utilisation.

En cas de perte de mot de passe Gmail propose, lors de la création du compte, d'indiquer une réponse à une question pour s'identifier, utiliser de préférence l'option « rédiger une question personnalisée » le piratage par « dictionnaire » (tentatives de réponses à des questions répertoriées) sera ainsi beaucoup plus ardu (les pirates doivent trouver la question et la réponse).

N'utiliser un compte de messagerie Gmail que pour des données peu sensibles.

Campagnes de revendications :

Exiger de Google des CGU, courtes, lisibles, compréhensibles par tous les utilisateurs pour chaque application et notamment Gmail. En effet pour lire les CGU il faut sans cesse se reporter d'un lien à un autre.

https://secure.eff.org/site/Advocacy?cmd=display&page=UserAction&id=433

Recommandations

Lire les conseil du Secrétariat général de la Défense nationale et de l'Agence nationale de la sécurité des systèmes d'information: http://www.securite-informatique.gouv.fr/gp_article74.html
Insister auprès des pouvoirs publics (nationaux et européens) et des autorités de protections des données personnelles pour que Google soit soumis au droit européen.

RESEAUX SOCIAUX

Myspace

Technologie utilisée	Il s'agit d'un site web de réseautage social créé aux Etats-Unis, mettant gratuitement à disposition des membres un espace web personnalisé, permettant de présenter diverses informations personnelles et d'y tenir un blog. Il propose également un système de messagerie et permet de publier des photos. Fondé en 2003 par Tom Anderson et Chris DeWolf, MySpace a été racheté par le groupe de Rupert Murdoch, News Corp en juillet 2005. Même si MySpace peut être utilisé afin de rester en contact avec des personnes ou d'en rencontrer de nouvelles, il s'agit avant tout d'un réseau musical permettant de promouvoir des talents et de partager de la musique. L'utilisateur entre en contact gratuitement avec d'autres utilisateurs (amis et réseaux de personnes constitués autour de la région, de l'école ou université, de l'entreprise ou de centres d'intérêt définis par l'utilisateur) et de partager avec eux divers documents multimédias (films, photos, textes…).
Pays d'utilisation	France, monde
Législation	Loi fédérale américaine. • Myspace a adhéré au système *Safe Harbour* qui répond à certains principes de la directive européenne. • Notons que les sites internet comme MySpace ne peuvent être tenus responsables pour le contenu mis en ligne ou pour toute mauvaise action commise par des individus qui visite leur site. Conditions d'utilisation de MySpace sur : http://www.myspace.com/index.cfm?fuseaction=misc.privacy • Un projet de loi aux États-Unis, le *Deleting Online Predators Act* (Dopa), a été déposé en 2006 devant le Congrès. Il vise à limiter l'accès des enfants aux réseaux sociaux dans les écoles et les bibliothèques. Cependant ce genre d'initiative n'offre pas de garantie d'atteindre son but car les enfants ont beaucoup d'autres moyens d'accéder à ces sites. • **« Myspace Suicide Case »** rendu par une Cour fédérale des Etats-Unis en novembre 2008. Lori Drew, 49 ans, a été condamné pour avoir violé les conditions d'utilisation du site Myspace en se faisant passer pour un jeune homme de 16 ans. En effet le site exige que les informations fournies soient vraies. L'impact de ce cas a été considérable puisqu'il a permis d'étendre la loi sur les « Fraudes et abus informatiques » de 1986 aux réseaux sociaux alors qu'elle était originellement dirigée contre les hackers. C'est le **premier cas de répression d'un « cyber-harcèlement »** qui avait conduit au suicide d'une jeune fille.
Statistiques concernant la population	Entre 16 et 35 ans. En 2009 les mineurs représentent 12% alors qu'il y a un an ils représentaient 25%. La tranche des 34-54 représente 41% contre 32% il y a un an, l'attrait pour les sites communautaires étant de plus en plus large. L'attrait des sites communautaires est de plus en plus large. Lancé en 2003 les jeunes ont commencé à véritablement s'y intéresser en 2005. Notons que 33% des utilisateurs ne se connectent qu'une fois par semaine.

Contenu du fichier	Myspace fait partie de l'initiative Data Availability. En pratique, Data Availability permet à un utilisateur de partager les données contenues dans son compte Myspace avec d'autres sites de son choix. Les membres de Myspace pourront ainsi partager les informations de leur profil, leur liste d'amis ou encore les photos et vidéos qu'ils ont mis en ligne. Myspace limite pour l'instant l'expérience à une poignée de gros sites (Yahoo, Ebay, le site de partage d'images Photobucket et le site de micro-blogging Twitter).
Durée de conservation	Pas d'information. Cependant, il existe une tendance générale à réduire la durée de conservation des données personnelles.
Qui détient les données ? **Qui y a accès ?**	Myspace est juge des fichiers et peut partager les données personnelles des utilisateurs avec d'autres sites. MySpace prévoit d'offrir une application gratuite de notification parentale permettant aux parents des jeunes internautes surfant sur MySpace d'utiliser un logiciel nommé **Zephyr**, pour déterminer quel nom, âge et lieu de domicile donnent leurs enfants sur leurs comptes MySpace.
Droit de regard et rectification	• Possibilité de bloquer l'accès à son profil. Si le profil n'est pas bloqué tout le monde peut y accéder (sans restrictions d'ordre géographique par exemple). • E-mail et adresse ne sont visibles que par les administrateurs. • Les utilisateurs peuvent publier des photos, ajouter des chansons/vidéos. • Possibilité de bloquer certaines personnes.
Dangers	• Concernant la publicité, il existe une option « opt-out » cependant, celle-ci est tellement cachée, qu'elle est difficile à trouver. La vente et l'usage des informations personnelles ne sont pas autorisés ; seule la publicité ciblée l'est. L'exposition est assez importante car une course au nombre de contacts semble exister, donc, il n'y a pas vraiment de tri dans les contacts. • Espionnage et enquêtes. • Délinquance sexuelle ; plusieurs cas ont déjà été appréhendés sur Myspace. • Droit à l'image et à la vie privée.
Campagne	Pas de campagne visant spécifiquement MySpace en France mais une étude faite par Reporters sans frontières, « *Les ennemis d'Internet* ». Réaction pour dénoncer le fichage effectué par Myspace, notamment via des articles de presse ou des groupes de mécontents sur le site même.
Recommandations	Mener des campagnes auprès des pouvoirs publics (nationaux et européens) et des autorités de protections des données personnelles pour que Myspace soit soumis au droit européen. Par ailleurs demander la possibilité pour les utilisateurs de réseaux sociaux : • d'une clôture définitive du compte incluant une suppression de toutes les données personnelles partagées ; • de rendre les profils des utilisateurs inaccessibles par défaut aux moteurs de recherche.

EVENEMENT DE LANCEMENT DE LA BD « SOUS SURVEILLANCE »
PRESENTATION DU PROJET DE PROTECTION DES DONNEES PERSONNELLES

JEUDI 22 AVRIL 2010 DE 16H A 19H A LA CANTINE

Le projet européen de protection des données personnelles

Présentation :

- Etat des lieux sur la protection des données personnelles ;
- les Tic dans la vie des jeunes et les enjeux de la sensibilisation ;
- présentation de la BD et le flipbook sur écran ;
  les usages de cet outil.

Une « société de surveillance » : les atteintes à la vie privée

Débat avec :

- Dominique Cardon, chercheur ;
- Jean-Pierre Dubois, universitaire, président de la LDH ;
- Noé Leblanc, journaliste ;
- Elisa Quillatre, juriste spécialisée en droit des NTIC ;
- Jean-Baptiste Thomas-Sertillange, avocat spécialisé en droit des NTIC.

Exposition des planches originales de la BD

Pause gourmande

La Cantine est le premier espace de travail collaboratif en réseau (« coworking space ») à Paris et Ile-de-France, relié à d'autres structures en France, en région, ou à l'étranger (San Francisco, Barcelone, Sao Paulo, etc...), conçu pour le travail collaboratif, facilite les coopérations fluides. De plus, la Cantine s'ouvre aux réseaux français et internationaux qu'ils soient des lieux de co-working, des plateformes artistiques, des lieux alternatifs, des pôles de compétitivité, des laboratoires de recherches spécialisés, des écoles ou des universités.

La cantine a pour but de faire se croiser des mondes qui travaillent dans des lieux éclatés afin de mutualiser les moyens et les compétences entre développeurs, entrepreneurs, usagers, artistes, chercheurs et étudiants. C'est donc un lieu de rencontre, d'informations, d'échange et de complémentarité entre des acteurs éclatés, axé sur l'intelligence collective.
Espace pluriel de création, d'expérimentation et d'innovation, la cantine a pour vocation de créer l'environnement propice au fourmillement d'idées dans une atmosphère de liberté et de créativité, ainsi que de favoriser le développement de projets, de logiciels et d'applications informatiques, mais aussi de contenu éducatif, de blogs, de vidéos, de photos, d'audio et toute création numérique en ligne.

lacantine.org
12, galerie Montmartre, 151 passage Montmartre, Passage des Panoramas, 75002 Paris