Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

France rapport national LDH

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH,EDRi,AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

Décembre 2009

SOMMAIRE

SYNTHESE

Méthodologie

Pour mener à bien l'étude sur les quatre thèmes concernant la protection des données personnelles retenus lors du kick off de février 2009, la LDH a pu s'appuyer sur :

- le groupe de travail de la LDH, "Libertés et TIC" qui se consacre à l'étude des menaces que font porter sur les droits et les libertés l'utilisation de l'informatique, de l'internet des TIC en général il est composé de juristes, d'informaticiens d'experts ou de citoyens vigilants ;
- le travail réalisé pour le congrès de la LDH les 1er et 2 juin 2009, dont le thème était "*Société de surveillance, vie privée et libertés*" ;
- le service juridique de la LDH ;
- les différents combats, menés notamment avec l'association IRIS (**I**maginons un **r**éseau **i**nternet **s**olidaire), des syndicats (de magistrats, d'avocats, de médecins, de fonctionnaires des impôts), contre tous les projets attentatoires aux libertés ;
- le rapport d'information du Sénat intitulé "*La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*", rendu public le 3 juin 2009 ;
- le rapport annuel du forum des droits de l'internet ;
- le rapport de la Fing (**F**ondation **i**nternet **n**ouvelle **g**énération) ;
- des interviews d'experts et notamment d'Alain Weber (avocat), Dominique Cardon (sociologue), Christophe Aguitton (chercheur et militant syndical).
- Le rapport d'information de l'assemblée Nationale « Fichiers de police : les défis de la République »

A partir des thèmes retenus, les sujets ont été choisis en comité de suivi du projet. Le travail sur les fiches a été fait à partir des interviews, des recherches dans les différents documents, les bases de données juridiques et des données publiées sur internet. Suite au travail réalisé, les fiches ont été révisées par le service juridique.

Législation et règlements concernant la vie privée

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 (c'est la première autorité indépendante instituée en France) les libertés et droits fondamentaux, dont la vie privée, à l'égard des fichiers et traitement de données personnelles. La **C**ommission **N**ationale **I**nformatique et **L**ibertés (CNIL) 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 la révélation à l'opinion de l'existence de fichiers de police occultes et de la mise en place de techniques de profilage pour détecter les enfants « à risques » (médicaux ou sociaux) à partir du fichier GAMIN (**G**estion **A**utomatique de la **M**édecine **In**fantile), 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

LA LOI N°78-17 DU 6 JANVIER 1978 MODIFIEE EN 2004 RELATIVE A L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTES

Conçue sur des principes généraux, universels et intemporels, la loi du 6 janvier 1978 a fait l'objet d'une dizaine de modifications destinés à en préciser l'application dans certains domaines (recherche médicale par exemple). La dernière, en août 2004, de plus grande envergure a été adoptée dans le contexte de la mise en conformité avec la directive européenne du 24 octobre 1995. Mais sous couvert d'une mise en conformité, la nouvelle loi a considérablement amoindri le régime d'autorisation préalable qui donnait jusqu'à lors à la CNIL la compétence générale pour refuser la mise en oeuvre 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. Par contre la nouvelle loi a renforcé les pouvoirs de la CNIL en matière contrôle préalable dans des domaines sensibles relevant du secteur privé et lui a conféré un pouvoir de sanction.

Les deux premiers articles de la loi du 6 janvier 1978 posent le cadre de la protection des données personnelles. L'article 7 est consacré au droit à l'information préalable et 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*".

Article 1er définit le cadre de la loi :

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 (maintien de l'article d'origine repris dans les considérants de la directive européenne de 1995).

L'article 2 définit notamment les notions de données personnelles et des traitements concernés:

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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

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.

Au chapitre II les Articles 6 et 7 définissent les principes s'appliquant aux données personnelles :

Le principe de finalité : un traitement ne peut être mis en œuvre que pour une finalité déterminée, explicite et légitime.

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 : qui, constituent de fait un nouveau traitement justifient l'application du principe de finalité (doivent faire l'objet d'une autorisation).

C'est au chapitre III de la loi, que les missions et fonctionnement de la CNIL sont précisés (voir § DPA).

Hormis la loi Informatique et Liberté, d'autres textes viennent en préciser les conditions de mise en œuvre dans des domaines particuliers ou établir certaines dérogations à certains de ces principes. Ceux pertinent au regard du champ de la présente étude sont les suivants :

PNR : ***ART.7 DE LA LOI N° 2006-64 DU 23 JANVIER 2006 RELATIVE A LA LUTTE CONTRE LE TERRORISME*** autorise le ministre de l'intérieur à créer des traitements automatisés des données à caractère personnel (PNR et APIs) recueillies à l'occasion des déplacements internationaux. Quant aux douanes, c'est l'Art.65 du code des douanes qui leur permet de requérir ponctuellement les données PNR de certains vols.

Dans sa ***RESOLUTION N° 84 DU 30 MAI 2009*** le ***SENAT*** s'est prononcé sur la proposition de décision-cadre relative à 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 et notamment que la transposition de la directive soit encadré par la loi. (voir Annexe xx ?????)

Passeport biométrique : il a été institué par de simples décrets. Les décrets instituant les passeports électroniques (***DECRET N° 2005-1726 DU 30 DECEMBRE 2005***) puis biométriques (***DECRET N° 2008-426 DU 30 AVRIL 2008***) ont été attaqués par la LDH devant le Conseil d'Etat pour violation du principe de proportionnalité prévu par la loi Informatique et Libertés. (Voir annexe xx ????). Alors que ces passeports sont délivrés depuis juin 2009, l'examen de la requête est toujours en cours.

LA LOI N° 2004-575 DU 21 JUIN 2004 POUR LA CONFIANCE DANS L'ECONOMIE NUMERIQUE (LCEN)

La loi du 21 juin 2004[1] transpose la directive européenne du 8 juin 2000. Le texte législatif établit un droit français de l'internet et pose les règles relatives au commerce électronique. L'apport essentiel de la LCEN est qu'elle pose un droit général de l'internet, notamment en ce que :

- elle définit les communications sur l'internet en créant de nouvelles catégories légales ;
- elle établit un régime de responsabilité pour ses acteurs.

LA LOI N° 91-646 DU 10 JUILLET 1991 RELATIVE AU SECRET DES CORRESPONDANCES EMISES PAR LA VOIE DES COMMUNICATIONS ELECTRONIQUES

En droit français, existe le principe général de secret des correspondances. Il est consacré, dans le cadre des communications électroniques, par la loi du 10 juillet 1991. Publiée au Journal Officiel le 13 juillet 1991, cette loi a été modifiée à plusieurs reprises, tant par voie réglementaire que législative.

Comme le précise le texte, "*le secret des correspondances émises par voie de télécommunications est garanti par la loi. 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*". En outre, la loi définit la télécommunication comme "*toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil optique, radioélectricité ou autres systèmes électroniques*."

Il s'agit donc d'une rédaction très large qui peut englober la messagerie électronique dès lors que la correspondance revêt un caractère privé.

[1] Source JurisPedia - http://fr.jurispedia.org

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. La tendance est à la surveillance et à la suspicion généralisée.

LA LOI « CREATION ET INTERNET » DITE « HADOPI » (HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES DROITS SUR INTERNET) a pour objet de protéger les auteurs et les industries du divertissement du téléchargement illégal par les internautes.

La loi prévoyait que le repérage des « pirates » se ferait par des sociétés privées, les ayants droit et producteurs d'œuvres, qui signaleraient à la HADOPI les adresses IP des présumés « pirates ». C'est la Haute Autorité, (première autorité administrative indépendante créée pour **restreindre** les droits et libertés) qui obtiendra leurs coordonnées auprès des fournisseurs d'accès (FAI) et après une « riposte graduée » pourra prononcer des sanctions (coupure d'accès internet, amendes…). En juin 2009 le Conseil constitutionnel a censuré la possibilité de sanctions par une autorité administrative et demandé que ce soit un juge qui prononce cette sanction.

La nouvelle loi votée en septembre 2009 prévoit de confier au juge des référés le pouvoir de prononcer une suspension de l'accès internet pour une durée d'un an maximum, confiant aux agents de l'Hadopi le pouvoir de constater les infractions. L'abonné reconnu coupable, sera privé pendant un an de connexion internet, il ne pourra pas souscrire un autre abonnement sous peine d'une autre sanction (jusqu'à 30.000 euros d'amende et deux ans de prison pour atteinte "à l'autorité de la justice pénale"). 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 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, les sauvegarder les intérêts de quelques entreprises, les autorités publiques vont instaurer un système de suspicion généralisée, pour surveiller les citoyens, collecter leurs données personnelles et ainsi de compromettre 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 t**el 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.**

LOPPSI-2 LOI D'ORIENTATION ET DE PROGRAMMATION POUR LA PERFORMANCE DE LA SECURITE INTERIEURE

En cours de discussion en début 2010, cette loi renforce encore la surveillance des citoyens.

La loi 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 croiser tous les renseignements disponibles pour lutter contre tous types de délinquance et notamment la pédopornographie. Pour cela ce fichier contiendra toutes sortes de données.

La LDH a tenu à alerter les élus sur la dangerosité de ce projet (11 février 2010) :

Vers le contrôle social total. 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.

C'est la multiplication des systèmes de vidéosurveillance, y compris désormais des manifestations, alors que toutes les expériences étrangères concluent à leur inefficacité dans la plupart des cas ; l'interconnexion des fichiers de police alors que la CNIL a établi que ces fichiers sont truffés d'erreurs ; le filtrage policier des sites Internet et la chasse aux internautes ; la création d'une justice virtuelle par la systématisation de la visioconférence pour les auditions de détenus ou d'étrangers en rétention administrative.

C'est surtout la légalisation des « mouchards électroniques » introduits dans les ordinateurs personnels à l'insu des citoyens espionnés. Et le super-fichier « Périclès » pourra croiser tous les renseignements fournis par ces fichiers, par les puces téléphoniques, les factures de paiement en ligne, les numéros de pièces d'identité…

[…]

La Ligue des droits de l'Homme invite chaque parlementaire à mesurer la responsabilité qui est la sienne devant le changement de société dont ce projet de loi est porteur. Elle appelle les citoyens à refuser d'être traités comme de présumés délinquants sous contrôle étatique permanent, dans les moindres recoins de leur vie privée.

Autorité de protection des données

LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES

Pour la CNIL, « *L'informatique doit respecter l'identité humaine, les droits de l'homme, la vie privée et les libertés ».*

La Commission Nationale Informatique et Liberté (CNIL) a été créée par la loi dite Informatique et Libertés en 1978. Elle est composée de 18 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 par ailleurs sénateur, il peut donc émettre au sein de la CNIL des avis critiques sur des projets de loi et voter différemment au Sénat. 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, à savoir 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[2] :

- **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. La CNIL informe également 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

Mais en 2004, la France qui était tenue, de remanier la loi de 1978 pour se mettre en conformité avec la directive européenne du 24 octobre 1995 sur la protection des données personnelles, a modifié les compétences de la CNIL : elle ne peut plus s'opposer à la création de fichiers de police, mais rend un avis consultatif, publié au Journal officiel qui n'influera pas sur leur création. Par ailleurs, la loi de 2004 a créé la profession de "correspondants informatique et libertés" dans les entreprises permettant ainsi 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 dans ce cadre

Ces allégements de procédure sont théoriquement compensés par l'attribution à la CNIL de nouveaux pouvoirs d'investigation et de sanctions. La Commission peut ainsi infliger des amendes - jusqu'à 300

[2] Informations prises à partir du site http://wiki.univ-paris5.fr/wiki/CNIL

000 euros - en cas de manquement Toutefois son manque de moyens rend ces investigations en nombre très faibles (quelques deux cents par an.

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.*
En 2008, ce sont 71 990 fichiers qui ont été déclarés, 4 244 plaintes ont été déposées, 218 contrôles effectués, et 2 516 accès aux fichiers de police demandés. Soit 116 % de plus qu'en 2007,
3 500 demandes n'ont pas pu être traitées !

Bien que 12 emplois aient été créés, la CNIL manque de moyens pour traiter les problèmes posés par la vidéosurveillance, les projets de loi tels Hadopi, la loi sur l'orientation et la performance de la police (LOPPSI), les réseaux sociaux, le fichage des élèves, les fichiers mis en œuvre sans autorisation, et les problèmes posés par les fichiers de police contenant des milliers d'erreurs.

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 d'inconscients**.

La CNIL est une instance qui a longtemps bénéficié d'une certaine confiance des citoyens, toutefois depuis qu'une partie de ses pouvoirs lui ont été retirés en 2004, des défenseurs des libertés considèrent qu'elle n'est plus audible au point d'occuper ses locaux en décembre 2007.

Tandis que des associations demandent le renforcement de son caractère pluraliste et démocratique notamment par le choix des cinq personnalités qualifiées sur proposition des syndicats et des associations de défense des droits de l'Homme.

Lors de son congrès 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;* ***la CNIL doit en particulier retrouver les pouvoirs qu'on lui a retirés en 2004*** *;* »

LA COMMISSION NATIONALE DE CONTROLE DES INTERCEPTIONS DE SECURITE (CNCIS)

C'est une 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 à plusieurs reprises, et notamment par la loi du 23 janvier 2006.

« Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. *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.* »

Les interceptions légales de correspondances émises par la voie des « *communications électroniques »* sont de deux types, judiciaires et de sécurité.

En application de l'article 15 de la loi, la Commission nationale reçoit les réclamations des particuliers, procède en toute indépendance aux contrôles et enquêtes qui lui paraissent nécessaires à

l'accomplissement de sa mission et s'attache à nouer tous contacts utiles à son information ; elle peut à tout moment adresser au Premier ministre une recommandation tendant à ce qu'une interception soit interrompue.

En outre, la Commission nationale est chargée, en application de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la loi contre le terrorisme, du contrôle des demandes de communication des données prévues par l'article L. 34-1-1 du code des postes et des communications électroniques.

http://lannuaire.service-public.fr/services_nationaux/autorite-administrative-independante_172128.html

Hormis ces deux autorités indépendantes, l'Etat a mis en place de nombreuses instances chargées de contrôler la sécurité des réseaux ou d'informer les citoyens sur la protection des leurs données personnelles. Voir en annexe de ce chapitre (page 18) : les instances officielles ayant un rapport avec la protection des données.

Sensibilisation aux questions de vie privée

Durant l'été 2008, une très forte mobilisation a eu lieu en France : 700 organisations et 250 000 individus se sont rassemblés contre la mise en place, par décret gouvernemental, d'un fichier dénommé EDVIGE (**E**xploitation **D**ocumentaire et **V**alorisation de l'**I**nformation **GE**nérale) susceptible de porter atteinte à la vie privée et aux libertés. Le Conseil d'Etat a censuré une partie du décret, suivant ainsi les arguments mis en lumière par les organisations et syndicats. Ainsi, le gouvernement a dû revenir en partie sur la finalité et le contenu du fichier.

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 les dispositifs répertoriés en annexe de ce document, dispositifs venus renforcer ceux mis en place au niveau de l'UE. Pour autant, les dispositions et outils existants ne suffisent pas à protéger nos données personnelles et nos vies privées dans un monde globalisé où les volontés politiques sont dirigées vers une plus grande surveillance du citoyen, une volonté d'assurer une forme de sécurité au prix des libertés - la lutte contre le terrorisme n'étant qu'un prétexte -, des intérêts industriels et commerciaux exploitant les avancées technologiques, influençant au besoin les décisions politiques pour leur profit - biométrie, RFID, vidéosurveillance, etc.

Au fil des projets gouvernementaux, les mobilisations ont été nombreuses pour combattre entre autres :

- le fichier STIC,
- la carte d'identité infalsifiable INES,
- le passeport électronique devenu passeport biométrique,
- le fichier ELOI,
- les fichiers SCONET et Base élèves premier degré,
- les fichiers EDVIGE, CRISTINA, et le FNAEG
- la vidéosurveillance
- les deux nouveaux fichiers remplaçant EDVIGE ("*Enquêtes administratives liées à la sécurité publique*" et "*Prévention des atteintes à la sécurité publique*"), créés par décrets du 16 octobre 2009, parus au Journal officiel le 18 octobre 2009[3]..

[3] Les nouveaux fichiers mentionnent notamment le fait que les mineurs pourront être fichés dès l'âge de 13 ans, les personnes pourront être fichées à partir du simple fait qu'elles habitent une certaine zone géographique, l'appartenance syndicale, les opinions politiques, religieuses ou philosophiques pourront justifier en elles-mêmes qu'une personne ne puisse pas accéder à certains emplois (extrait du dossier de presse du collectif "Non à EDVIGE", 4 décembre 2009).

DES MOBILISATIONS A L'EFFICACITE INEGALE

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

- **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*".

Suite à la mobilisation des associations, notamment ***R****ésistance à l'****a****gression* ***p****ublicitaire* (RAP), la RATP a annoncé au mois de juillet 2009 qu'elle renonçait au déploiement des caméras analysant le comportement des usagers passant devant ces nouveaux écrans publicitaires. Les associations ont toutefois insisté pour que la CNIL poursuive l'étude détaillée de ce type de dispositifs et se prononce sur leur illégalité et leur illégitimité.

- **Fichier ELOI**

Par arrêté du ministre de l'Intérieur, a été créé le fichier ELOI destiné à "*faciliter l'éloignement des étrangers se maintenant sans droit sur le territoire*". Ce texte, paru le 18 août 2006, a été contesté par plusieurs associations devant le Conseil d'Etat. Par décision rendue le 13 mars 2007, le Conseil d'Etat a annulé l'arrêté ministériel estimant qu'un tel outil devait donner lieu à un décret et passer par la CNIL.

Face à cette mobilisation, il apparaît que le gouvernement a été contraint de "battre en retraite" sur un certain nombre de points, notamment en ce qui concerne le fichage des visiteurs d'étrangers retenus en centre de rétention. Un décret du 26 décembre 2007 a alors créé la seconde version du fichier ELOI, version expurgée de ces dernières dispositions. Cependant, des points soulevés dans le premier recours demeurent. Ainsi une nouvelle requête en annulation a été déposée par les associations devant le Conseil d'Etat. Le rapporteur public a recommandé l'annulation partielle du décret, à savoir :

- la deuxième finalité du fichier, c'est-à-dire l'établissement de statistiques relatives aux mesures d'éloignement et à leur exécution ;
- l'enregistrement du numéro AGDREF dans les données relatives à l'étranger 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.

Le Conseil d'Etat a effectivement annulé les 2 derniers points le 30 décembre 2009.

- **BASE ELEVES**

Selon le ministère de l'Education Nationale, l'application informatique "Base élèves premier degré" permet la gestion administrative et pédagogique des élèves de la maternelle au C.M.2 dans les écoles publiques ou privées. La base élèves est expérimentée depuis 2005 en lien avec la Commission nationale de l'informatique et des libertés (CNIL) et est en cours de généralisation en 2009 selon le contenu fixé par l'arrêté ministériel du 20 octobre 2008.

Les renseignements censés être fournis par ce fichier étaient au départ considérables puisqu'ils concernaient la culture d'origine, la nationalité ou encore la date d'arrivée sur le territoire, la langue parlée à la maison, l'intégralité du parcours pédagogique (redoublement, absentéisme, suivi par un réseau d'aide etc.) et des indications aussi personnelles que la façon dont l'enfant se rend à l'école (accompagné ou non…).

Dans un premier temps peu de parents d'élèves ont réagi, ignorant ce fichier. Puis des directeurs chargés d'enregistrer ces données ont décidé de refuser, s'inquiétant des accès donnés notamment

aux maires des communes aux inspecteurs d'académie et du manque de sécurité de ces accès. La mobilisation s'est amplifiée notamment par une pétition, des plaintes déposées par des parents. Elle a porté ses fruits puisque le Ministère est revenu sur le contenu. Sur son site il se sent obligé de préciser ce que la base de données ne comporte pas (la nationalité et l'origine des élèves et de leurs responsables légaux la situation familiale, la profession et la catégorie sociale des parents, l'absentéisme, les besoins éducatifs particuliers, la santé des élèves, les notes et les acquis de l'élève).

Toutefois, l'attribution d'un identifiant élève et une base de données nationales de ces identifiants inquiète toujours les défenseurs des libertés.

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* ». Le comité de l'ONU présente deux exigences : que les parents aient un droit de rectification et d'effacement du fichier et que les accès à celui-ci soient véritablement sécurisés. Ce sont précisément les demandes portées depuis des mois par les parents d'élèves et les défenseurs des droits de l'Homme.

Ainsi le Comité des droits de l'enfant de l'ONU a exprimées de nombreuses réserves à propos du fichier « base élèves ». Le comité, dans son avis prononcé le 11 juin 2009, 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 sont mobilisés dans ces combats qui restent le fait de militants attentifs à tous les projets de lois mais aussi à toutes les innovations destinées à augmenter la « sécurité des citoyens », à faciliter la vie courante, mais qui comportent une intrusion dans la vie privée.

NOUVELLES APPROCHES DE LA PROTECTION DE LA VIE PRIVEE

Ainsi 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 un chaine 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, la 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 qu'ils ont de n'avoir rien à se reprocher les incite à ne rien cacher.

Il semble que ce soit dans la lutte contre la vidéosurveillance que l'on trouve le plus de mobilisations, peut-être parce qu'elle est parfois visible et fait l'objet d'annonces par les pouvoirs publics.

A propos des thèmes étudiés pour le projet

Les principaux problèmes relevés dans les thèmes étudiés :

Mobilité et transports

Les risques de traçage :

Les utilisateurs des Passe 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, du manque de sécurité de ces puces RFID sur lesquelles les informations sont stockées et du risque de traçage du au fait que leurs trajets peuvent être enregistrés. La RATP ne fait aucune promotion de la version du passe « anonyme ».

La géo localisation induit un très fort risque de traçage notamment des salariés ce qui est une atteinte à leur vie privée mais aussi au droit du travail.

L'identité biologique

Non seulement 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 de celui-ci. Par ailleurs le fichier lié à la délivrance du passeport pose le problème de constitution d'une base de données de huit empreintes digitales et de données ethno-raciale (photo) dont la mise à disposition (aux enquêteurs de polices) en modifie la finalité qui a justifié sa constitution. Enfin la biométrie change radicalement à l'échelle de l'histoire 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 l'accoutumance recherché par les pouvoirs publics à ce type de contrôle.

Communications interpersonnelles

Les problèmes posés par l'utilisation de la messagerie électronique sont d'une part les résultats soit de la vente soit de la non protection des coordonnées de l'abonné qui sont alors utilisées par des sociétés de marketing pour des sollicitations commerciales. Par ailleurs les données peuvent être piratées et il existe un risque d'usurpation d'identité. Lorsqu'elle est gérée par un FAI la messagerie fait l'objet de rétention des données de connexion et de certains éléments des courriels par le FAI, dans le cadre de la lutte contre le terrorisme. Concernant les téléphones portables s'ajoute le risque de géo localisation à l'insu de l'abonné.

Réseaux sociaux

Les principaux problèmes relevés sont les atteintes à la vie privée qui résultent le plus souvent d'un manque de connaissance des paramétrages des profils qui permettent de protéger ses données personnelles en ne rendant public que certaines informations publiées, les autres étant partagées avec un nombre restreint de connaissances. Les révélations très médiatisées de problèmes advenus à certains abonnés de réseaux sociaux ou certains blogueurs ont sensibilisés quelques adeptes qui de plus en plus réclament un droit à la fois à la récupération de leurs données et à l'effacement de leurs données lorsqu'ils souhaitent changer d'opérateur.

Par ailleurs les SNS américains refusent obstinément de considérer que le droit européen s'applique 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 les sociétés américaines le droit européen.

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 recueillis 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'eller 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.

ANNEXES

LES INSTANCES OFFICIELLES AUTRE QUE LA CNIL AYANT UN RAPPORT AVEC LA PROTECTION DES DONNEES

SECRETARIAT GENERAL DE LA DEFENSE NATIONALE (SGDN) [GENERAL SECRETARIAT FOR NATIONAL DEFENCE]

Une de ses missions principales est de renforcer la sécurité des réseaux et des systèmes d'information de l'Etat et des services publics. Le SGDN contribue, en liaison avec les grands opérateurs, à l'identification et à la surveillance des risques affectant la sécurité des systèmes d'information : intrusions dans les réseaux, interceptions malveillantes de communications, prolifération des virus informatiques, manipulation de l'information. Le SGDN mène des actions de sensibilisation des autorités sur tous les événements et les fragilités informatiques qu'il peut identifier.

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI)

L'ANSSI dépend du SGDN. Créée en juillet 2009 sous la forme d'un service à compétence nationale rattachée au secrétaire général de la défense nationale. L'Agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information pour la mise en œuvre de la politique de défense contre les attaques informatiques.

A côté de son site officiel, l'ANSSI publie un portail de sécurité informatique : http://www.securite-informatique.gouv.fr . Mis en place en 2008, ce portail a pour objet de fournir des informations pratiques et des avis aux personnes privées et aux professionnels. Il contient : des alertes de sécurité, un glossaire sur la sécurité informatique, un guide et des recommandations au sujet des mots de passe, informe sur l'importance des pratiques de sécurité, etc. Il fournit, par ailleurs, de nombreux liens sur des organismes pour protéger les données.

CENTRE D'EXPERTISE GOUVERNEMENTAL DE REPONSE ET DE TRAITEMENT DES ATTAQUES INFORMATIQUES CERTA

Il s'agit d'un site gouvernemental qui publie la liste des vulnérabilités signalées par les éditeurs. Les références sont : http://www.certa.ssi.gouv.fr

AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES (ARCEP) [FRENCH TELECOMMUNICATIONS AND POSTS REGULATOR] - HTTP://WWW.ARCEP.FR

L'autorité de régulation des télécommunications (ART) avait été créée par la loi de 1996 pour réguler le secteur des télécommunications. Il s'agit d'une autorité administrative indépendante qui en 2005 s'est vue confier également la régulation des activités postales. Elle est en charge de la transposition des directives européennes en matière de communications électroniques.

OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITE LIEE AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (OCLCTIC) [CENTRAL OFFICE FOR THE FIGHT AGAINST CRIME RELATED TI INFORMATION TECHNOLOGY AND COMMUNICATION]

L'office central a été créé en 2000 au sein du ministère de l'intérieur, et plus précisément il est rattaché à la sous-direction des affaires économiques et financières de la direction centrale de la police judiciaire.

La lutte contre la cybercriminalité, et les fraudes aux cartes bancaires, recouvre le traitement judiciaire des infractions spécifiques à la criminalité liée aux nouvelles technologies et à celles dont la commission est facilitée ou liée à l'usage de ces mêmes technologies. Il assure aussi la formation, l'animation et la coordination de l'action des autres services répressifs, compétents en matière d'infractions liées aux technologies de l'information et de la communication ainsi que la coopération internationale - Europol, Interpol, G8.

DELEGATION AUX USAGES DE L'INTERNET (DUI) -

http://delegation.internet.gouv.fr

La DUI a pour mission de proposer les mesures nécessaires au développement de la société de l'information au bénéfice de tous et partout, notamment des mesures pour réduire la fracture numérique. Créée en 2003, la délégation est rattachée au ministre de l'Enseignement supérieur et de la recherche. Elle est chargée de développer l'accès à l'internet pour tous avec, entre autre des espaces publics numériques labellisés NetPublic, de favoriser la sécurité des personnes sur internet en général et la protection des mineurs en particulier - pilotage du programme européen Confiance, Tour de France des collèges et des écoles, etc. - ainsi que la formation et l'accompagnement aux TIC - opération internet accompagné, passeport internet multimédia, etc.

LES SITES INTERNET SOUS AUTORITE DE L'ETAT

SERVICE PUBLIC

http://vosdroits.service-public.fr/Fichiers, libertés, protection de la vie privée

Ce site explique le fonctionnement des accès aux fichiers contenant des informations personnelles, les principes, les droits des citoyens : droits d'accès, droits de rectification, d'opposition mais aussi les limites de ces droits - fichiers exclus des obligations CNIL etc. Des liens permettent d'accéder aux fiches pratiques ou aux courriers types proposés par la CNIL.

INTERNET SANS CRAINTES

http://www.internetsanscrainte.fr/accueil

Programme national de sensibilisation des jeunes aux bons usages de l'internet sur un site. Édité par la Délégation aux Usages de l'Internet (DUI) et Microsoft, ce programme est soutenu par l'Union européenne.
Le site "*internetsanscrainte.fr*" est le site officiel de prévention des risques d'usages de l'Internet pour les enfants. Les informations sont destinées aux enfants de 7-12 ans et aux jeunes de 12-16 ans ainsi qu'aux parents. On y trouve des brochures, des dessins animés pour les enfants, des quizz ainsi qu'un numéro d'appel pour faire part de ses inquiétudes à propos de l'internet.

PROTEGE TON ORDI

http://www.protegetonordi.com/

Ce site, résultat d'un partenariat public-privé entre les pouvoirs publics (la DUI), Microsoft et un collectif de partenaires, propose des conseils sous diverses formes et notamment de bandes dessinées pour adultes ou pour enfants sur le thème "*L'internet + sûr, on se mobilise ! […] pour vous aider à apprendre les gestes simples et indispensables afin de protéger votre ordinateur, protéger votre famille et vous protéger vous-mêmes*".

LE SITE "SURFEZ INTELLIGENT"

http://www.ddm.gouv.fr/surfezintelligent/

Objet du site : "*Comme dans la vie de tous les jours, il y a des règles de bonne conduite à suivre sur Internet pour pouvoir en profiter pleinement. Avec ses partenaires - acteurs* ***publics et privés*** *- le Secrétariat d'Etat en charge de la Prospective et du Développement de l'économie numérique vous propose quelques repères et bonnes pratiques indispensables pour "surfer" en toute sérénité*."
On y trouve une charte pour la promotion de l'authentification sur Internet afin de "*familiariser les internautes avec l'authentification*", distinguer l'authentification de l'identification, s'informer - "*reconnaissance des sites sécurisés, connaissance des données que certains interlocuteurs sont fondés à demander, données à ne communiquer sous aucun prétexte, lecture des contrats, obligations légales et contractuelles, accès aux données, etc.*"-inciter les internautes à acquérir de bons réflexes - "*sécuriser leur ordinateur : recours à des outils de protection, mises à jour régulières, gestion des moyens d'authentification, configuration des applications de sécurité, etc. […] ne pas cliquer sur un lien proposé par un spam*" -, ainsi que des "*Engagements réciproques des professionnels et des autorités publiques*".

QUELQUES ORGANISATIONS DE « VEILLE »

OBSERVATOIRE DE LA SECURITE DES SYSTEMES D'INFORMATION ET DES RESEAUX (OSSIR) [OBSERVATORY OF INFORMATION SYSTEMS AND NETWORK SECURITY] -http://www.ossir.org

L'OSSIR est une association qui regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux, qui organise annuellement la *Journée Sécurité des Systèmes d'Information*. Cette réunion annuelle réunit des experts, des professionnels sur tous les aspects de la sécurité - technique et législative - des systèmes d'information. En 2008, le thème était : « *Anonymat, vie privée et gestion d'identité... »* avec une présentation de la notion de "carte d'identité blanche", sur le thème "*Principes et technologies de protection de la vie privée sur l'Internet*".

FING - FONDATION INTERNET NOUVELLE GENERATION

http://fing.org/

Cette fondation, créée en 2000, compte dans ses membres à la fois des experts, des grandes entreprises, des start-ups, des laboratoires de recherche, des universités, des collectivités territoriales, des administrations. Elle assure un travail de veille sur les technologies, au croisement de la société, l'économie et la technologie. 3 domaines : veille et prospective / programmes d'actions / innovation ouverte. Ses objectifs annoncés sont :

- Jouer un rôle décisif dans l'émergence d'idées et de projets innovants ;
- Mobiliser les acteurs autour des cycles technologiques à venir ;
- Intervenir dans les nouveaux débats éthiques et sociétaux ;
- Faciliter l'innovation par l'usage.

Cette fondation travaille sur le thème « *Identités actives »* : l'identité numérique est le pivot, le fédérateur de la plupart des nouveaux services, des nouvelles pratiques qui émergent aujourd'hui sur l'internet (sur les blogs, réseaux sociaux, "*web 2.0*", fédération d'identités, portfolios, cartes multiservices, services composites, communautés, univers virtuels…). La question de l'anonymat ou "pseudonymat" est analysée et discutée sur le blog du site.

Elle travaille sur la question de savoir s'il faut mettre en place une **"loi Informatique et libertés 2.0"** en essayant de répondre à la question : "*si l'on met à part les évolutions (normales en 30 ans) internes au champ "Informatique & libertés" défini depuis 30 ans, ou encore les difficultés d'application - y a-t-il des éléments qui changent radicalement le contexte par rapport à 1978 : des pratiques (individuelles, collectives, d'entreprises ou d'administrations) très neuves et irréductibles à celles que nous connaissions ? Des techniques qui transforment le paysage ? Des échelles si différentes de celles de 1978 qu'elles changent la nature des phénomènes concernés ?... "*

LE FORUM DES DROITS SUR L'INTERNET - http://www.foruminternet.org/

Se définit comme "Trait d'union entre le public et le privé, le Forum est une réponse originale à la question de la régulation d'un univers en évolution permanente.". Le Forum compte près de 70 membres adhérents répartis en deux collèges, acteurs économiques et utilisateurs, composés de personnes morales, de personnes publiques ou de personnes issues de la société civile.
Il publie des conseils aux internautes, adolescents, parents, bloggeurs etc., sous différentes formes : bande dessinée, fiches, guides etc.
Le forum publie également des recommandations élaborées par différents groupes de travail, notes et des jurisprudences sur différents sujets liés à l'internet.

IMAGINONS UN RESEAU INTERNET SOLIDAIRE - IRIS

http://www.iris.sgdg.org/

Créée le 4 octobre 1997, l'association IRIS a, comme elle se définit elle-même, « *pour ambition d'agir sur le développement de l'internet dans le sens de plus d'égalité, de partage et de solidarité* ».
Ses principaux axes de réflexion et d'action sont :

- d'intervenir pour le développement d'une infrastructure de service public permettant l'accès pour tous à une connectivité permanente ;
- de permettre à tous la production de contenus et leur communication publique indépendamment des intermédiaires ;
- de lutter pour la pérennité de secteurs non-marchands sur internet.

En France, IRIS est membre du ***COLLECTIF DELIS (DROITS ET LIBERTES FACE A L'INFORMATISATION DE LA SOCIETE*** : www.delis.sgdg.org.

A l'échelle européenne, IRIS est membre fondateur de la fédération EDRI (**E**uropean **D**igital **Ri**ghts : www.edri.org).

Au plan international, IRIS est membre de la coalition GILC (**G**lobal **i**nternet **l**iberty **c**ampaign : www.gilc.org).

L'association est active au plan national en ce qu'elle procède à des auditions et des consultations institutionnelles. Elle sensibilise le milieu associatif et syndical aux enjeux politique et sociaux d'Internet. Iris publie également des rapports et analyses, organise des conférences et des débats. Au niveau européen, Iris participe à des groupes de travail de la Commission européenne sur les contenus illégaux et offensants sur Internet et sur la cybercriminalité. Enfin, au niveau international, l'association intervient auprès du Conseil de l'Europe et de l'Unesco, notamment dans le cadre de la coalition GILC.

Mobilité et transports

PASSE NAVIGO

THEME	PASSE NAVIGO Titre de transport, muni d'une carte à puce, utilisé par les usagers des 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 et fichier de stockage des données collectées. 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 (peinture, neige, etc.). L'étiquette est composée d'une puce et d'une antenne intégrée dans un support, carte plastique dans le cas du Passe Navigo. Elle est lue par un lecteur qui capte et transmet les informations stockées sur la puce. Il existe trois types d'étiquettes RFID : * Les étiquettes à lecture seule unique, * Les étiquettes à lecture multiple, * Les étiquettes à lecture et réécriture. Et, deux grandes familles d'étiquettes RFID : * Les étiquettes actives, reliées à une source d'énergie embarquée (type télépéage autoroutier). * Les étiquettes passives, utilisant l'énergie provenant d'un lecteur-émetteur. Ces étiquettes à moindre coût sont généralement plus petites et possèdent une durée de vie quasi-illimitée. La puce RIFD du passe NAVIGO est une RFID passive de technologie CALYPSO répondant aux normes standard ISO 7816-1, 2, 3, 44 et CEN 1545. Elle transmet les informations qu'elle contient mais ne peut pas en recevoir. 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-validateur 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. Il n'est pas possible de connaître le trajet complet effectué. 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

- [4] ISO-7816-1 : caractéristiques physiques de la carte ; ISO-7816-2 : emplacement des contacts électriques ;
- ISO-7816-3 : nature des signaux électriques et protocole de transmission entre le terminal et la carte ;
- ISO-7816-4 : organisation des données et sécurisation ;

Population concernée :	Potentiellement toute la population, pas de restriction d'âge et/ou de condition. Néanmoins, les populations les plus concernées sont : - les salariés qui se déplacent tous les jours de leur domicile vers leur lieu de travail. - les collégiens et les étudiants pour rejoindre leur lieu d'étude. Au 31 janvier 2009, Navigo comptait 4 536 000 clients (source ratp.fr) répartis de la manière suivante : • 2 498 000 cartes orange mensuelles ou hebdomadaires Il s'agit d'un titre de transport sous forme d'abonnement hebdomadaire ou mensuel pour se déplacer de manière illimitée dans des zones de son abonnement, en île de France. • 870 000 abonnements « intégrale » C'est un titre de transport sous forme d'abonnement de longue durée pour se déplacer de manière illimitée dans des zones de son abonnement, en île de France. • 779 000 abonnements imagine R Il s'agit d'un titre de transport destiné aux jeunes étudiants de l'île de France qui ont entre 12 et 25 ans. Valable 1 an, elle permet d'utiliser les différents transports en commun de la région. Pendant la semaine, son utilisateur peut librement se déplacer dans les zones définies par son abonnement. Le week-end, jours fériés et vacances scolaires, la carte est dite « dézonée », l'autorisant à se rendre dans toute l'île de France. • 389 000 abonnements Navigo découverte C'est un passe Navigo accessible depuis 2007 à tous les voyageurs, franciliens ou non, crée à la demande de la CNIL qui exigeait une version anonyme du passe navigo 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. Il se présente lui aussi sous la forme d'une carte à puce RFID, sans contact, il est associé à une carte nominative de transport intégrant une photo et l'inscription manuscrite de ses nom et prénom de l'usager. Il permet de charger des abonnements de courte durée carte orange. Mais il ne sera pas remboursé en cas de perte ou de vol, pas plus que les forfaits chargés dans sa puce, puisque aucune donnée nominative ne permettra de vérifier que l'usager les a bien acquittés.
% d'utilisation/de la population concernée globalement et chez les jeunes	Pas de statistique fiable dans le rapport utilisation / âge de l'utilisateur
Tendance	Pas de statistique fiable.
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. Par ailleurs il est possible pour quiconque ayant le lecteur adéquat de lire le contenu d'une puce RFID à l'insu du porteur. S'il s'agit de la puce du passe Navigo qui comporte des données personnelles permettant ainsi d'identifier à distance son porteur il est possible de pister les individus dans tous les actes de la vie quotidienne En France, la Commission Nationale de l'Informatique et des Libertés (CNIL) a d'ores et déjà placé les étiquettes à RFID parmi les technologies à risques pour les libertés individuelles, estimant qu'elles constituent des données personnelles au sens de la loi informatique et libertés de 1978. 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	Source : Conditions générales d'utilisation 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) visibles en annexe Les données collectées font l'objet d'un traitement automatisé dont la finalité est la gestion de l'abonnement carte orange et de la demande de Passe Navigo.
Fichier associé et date de création	Référence inconnue création 2003
Finalité du fichier	La gestion, la délivrance et l'utilisation des titres de transport : - gestion des abonnements et délivrance des titres de transport plein tarif, à tarif réduit ou même gratuits ; - gestion des opérations du service après vente et des réclamations clients. La gestion et le suivi des relations commerciales La gestion de la fraude : - détection de la contrefaçon et de la fraude technologique et instruction des dossiers; - gestion des cartes invalidées suite à une perte, un vol ou suite à un incident de paiement.; - gestion des cartes invalidées suite à la détection d'un usage abusif (par exemple : détection de plusieurs dizaines de passage avec un même passe) ; La réalisation d'analyses statistiques d'utilisation des réseaux : - analyses statistiques : o du trafic ; o de la nature des titres de transport délivrés ; o de la clientèle ; o d'utilisation par type de titres de transport. La mesure de la qualité du fonctionnement du système : - analyses des problèmes techniques liés à la carte, aux validateurs; détection des anomalies fonctionnelles du système d'information.
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. En 2006 un internaute a eu accès aux fiches d'abonnés Navigo l'adresse internet de chaque formulaire reprenait une partie des chiffres du numéro de client. En modifiant ces chiffres dans le navigateur, l'internaute a réussi à accéder à 1.400 demandes d'adhésion intégrant la photo du client, ses nom, prénom, adresse postale, courriel et numéro de téléphone.
Durée de conservation ?	Pour la gestion : L'ensemble des données clients est conservé pendant la durée de la relation contractuelle, et à l'issue de celle-ci pendant deux ans à des fins commerciales et statistiques pour les clients et

	prospects. Pour les déplacements journaliers : Les données de validation contenant des informations relatives aux déplacements des personnes, associées au numéro de carte ou de l'abonné, élément renvoyant indirectement à l'identité d'un usager, pourront être conservées pendant 48h au maximum et aux seules fins de lutter contre la fraude technologique.
Droit de regard et de rectification ?	Les droits d'accès et de rectification définis au chapitre V de la loi du 6 janvier 1978 modifiée s'exercent auprès du ou des services que le responsable de traitement aura désignés.
Finalité cachée du fichier et détournements/ Risques	La Commission Nationale Informatique et Liberté 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 à moitié 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. Dans son avis du 8 avril 2004, la CNIL a exigé que le STIF mette en place une formule anonyme du passe Navigo rappelant « qu'il convenait de laisser aux usagers la possibilité d'utiliser un service de transports publics anonymement sans qu'il en résulte un surcoût par rapport au choix d'un passe nominatif » En réaction, le STIF a crée le 1er septembre 2007 le passe Navigo découverte anonyme. La CNIL s'est estimée satisfaite mais elle regrette néanmoins la mise en service tardive et payante de ce passe anonyme (coût : 5 euro). Afin de contrebalancer ce coût, le passe a une durée de vie de 10 ans. Le 6 janvier 2009, suite à diverses plaintes de consommateurs et des opérations de testing sur le terrain, la CNIL a estimé que « l'exercice du droit des usagers à se déplacer anonymement n'est pas garanti, les conditions d'information et d'obtention du passe Navigo découverte étant médiocres voire dissuasives. En effet, il est possible de noter un manque de sensibilisation du personnel concernant la vente de ce passe, l'absence régulière de documentation commerciale ainsi que des difficultés pratiques à l'obtenir au guichet).
Législation en application	
Loi	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, loi Informatique et Liberté du 6 janvier 1978 modifiée le 6 août 2004. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20090723.
Risques pour les libertés malgré l'encadrement par la loi	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 vidéo surveillance, la problématique Passe Navigo contournent 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 ….. »
Ces outils et le public jeunes et jeunes adultes	
Niveau auquel ils sont concernés ou importance de l'utilisation	Les adolescents et les jeunes adultes, étudiants ou salariés, sont comme l'ensemble des individus concernés par les possibilités de fichage, traçage et profilage.
Conscience des problèmes ou des risques encourus	Ils 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, à partir du Passe Navigo. La technologie RFID se développe très rapidement sans que le public soit informé des dangers potentiels en termes de traçage et de profilage de l'Etat et du secteur marchand. Il est urgent de communiquer sur le sujet auprès du public. 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)
Conclusions	
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 ?)

P N R

THEME	**PNR - PASSENGER NAME RECORD (enregistrement des données des passagers)**
Technologie utilisée	**Base de données et transmission de données par réseau**
Pays	Europe ⇔ Etats-Unis Des accords ont été conclus entre l'UE et le Canada et aussi entre l'UE et l'Australie.
Cadre d'utilisation	Il s'agit d'un accord Europe-USA. Dans le cadre de la lutte contre le terrorisme, les compagnies aériennes européennes doivent fournir pour chaque vol vers les USA, chaque transit ou simple survol, aux autorités américaines (Bureau des douanes et de la protection des frontières) un accès à leurs bases de données contenant les données personnelles des passagers concernant l'ensemble des détails du voyage. Ces informations sont collectées auprès des clients, au stade de la réservation commerciale par les agences de voyage ou les Cie aériennes et enregistrées par les systèmes de réservation communs à plusieurs Cie ou agences comme Amadeus. Elles permettent d'identifier l'itinéraire du déplacement, les vols concernés, le contact à terre (numéro de téléphone), les tarifs accordés, le numéro de carte bancaire du passager ainsi que les services demandés à bord tels que les exigences alimentaires spécifiques (végétarien, asiatique, cascher) ou des services liés à l'état de santé du passager, ainsi que les services durant le séjour (hôtel, location de véhicule etc.). Voir liste au § « Contenu du fichier ». Les autorités américaines exigent l'accès aux bases de données 72 heures avant chaque vol vers les USA. Les autorités reçoivent par ailleurs les données APIs, (Advance Passenger Information), complétées au moment de l'enregistrement et transmises au moment du départ du vol. Ces données concernent l'état civil le N° de passeport etc. Cette collecte sert à détecter sur la base de modèles de profilage la constitution d'un fichier de personnes à comparer à la « no fly list » ou à la « selectee list ». La **no-fly list** contient les noms des passagers qui, pour certains motifs, ne sont pas autorisés à voler. Les passagers sur cette liste se voient refuser les cartes d'embarquement La « **selectee list »** contient les noms des passagers qui présentent un risque supérieur à la normale et nécessitent donc des contrôles de sécurité supplémentaires pour eux et leurs bagages. De tels accords ont été signés avec le Canada, et l'Australie. Le Royaume-Uni s'est doté d'un tel système de surveillance avec des pays européens.
Population concernée	Tous les âges sont concernés. Aucune indication faisant état d'une restriction d'âge. Selon EUROSTAT, Entre 2003 et 2004 le nombre de passagers aériens entre l'Europe (à 25) et les USA a augmenté de 12%, soient plus de 45 millions de passagers aériens (sur 215.000 vols).Cette tendance reste à la hausse.
Fichiers générés et leur objet	L'administration américaine n'a communiqué que des informations partielles à ce sujet. Il semble qu'il y ait trois fichiers : - No fly list : Interdiction du territoire des Etats Unis. - Selectee list : Fichiers d'attente de vérification avant décision. - Fichiers des données collectées (PNR). Ce dernier n'est pas transparent. Les données collectées sont conservées pendant au minimum 15 ans sans certitude de destruction au delà de ce délai. Un PNR est créé au moment d'une réservation auprès d'une agence de voyage ou d'une compagnie aérienne. Il permet de faire, selon le choix des voyageurs, une réservation pour un vol ou pour un itinéraire complet, y compris avec réservation d'hôtel et de voiture, pour une personne ou pour plusieurs personnes voyageant ensemble. Il y a donc constitution de fichiers auprès de ces différents acteurs par le biais des services de plateforme de réservation comme AMADEUS en Europe vers lesquels sont acheminés tous les PNR et qui assurent ainsi la transmissions des données pertinentes aux différents acteurs concernés. Chaque personne se rendant aux USA est dans l'obligation de remplir en ligne, un formulaire sur

	le site de l'ambassade américaine. A l'arrivée sur le sol américain, le passage à l'immigration est obligatoire et à ce moment-là des photos du passager sont prises ainsi que ses empreintes digitales.
Contenu du fichier	La liste complète des données que peut contenir un PNR selon la nomenclature de l'association internationale de transport aérien (IATA) est disponible sur le site de la CNIL (www.cnil.fr). Le fichier contient notamment, de manière non exhaustive : - nom et prénom du passager, - résidence, - coordonnées téléphoniques, - adresse électronique, - mode de paiement (numéro de carte de crédit, adresse de facturation, prix du billet), - informations APIS - tels que le numéro du passeport, - date de naissance et nationalité, - données OSI (zone de saisie libre : mention des demandes diverses exprimées par le passager, comme la fourniture d'une chaise roulante à l'arrivée, données SSI/SSR - demande de services spéciaux en fonction des préférences alimentaires, de l'état de santé ou de l'âge, par exemple : végétarien, diabétique, sans sel, sans porc, assistance médicale, - (dans le fichier des compagnies aériennes observations générales relatives à d'éventuels incidents survenus sur les vols précédents : altercations, abus d'alcool, etc.), - statut du voyageur -classe économique, affaire, grand voyageur, miles parcourus), - date de réservation du voyage, - date prévue du voyage, - date d'émission du billet, - itinéraire complet du voyageur, - passager sans réservation, - passager répertorié comme défaillant (absent lors de l'embarquement malgré une réservation), - agent et agence de voyage ayant vendu le billet, - informations relatives au siège occupé (à gauche, à droite, à l'avant, à l'arrière de l'avion), - historique des changements apporté dans le fichier PNR.
Durée de conservation des données	Les données PNR des GDS sont conservées un mois après le vol et 3 mois en archives. Les données recueillies par les autorités américaines sont conservées 15 ans sans qu'il n'y ait de garantie quant à leur destruction.
Qui détient le fichier / qui y a accès	Les agences de voyages, les compagnies aériennes et les GDS Les autorités américaines
Droit de regard et rectification	Fichier des autorités américaines - Il existe des protections administratives à l'ensemble des données PNR, indépendamment de la nationalité ou du pays de résidence de l'intéressé. - En outre, il existe un système de recours pour les personnes souhaitant obtenir des informations sur les PNR les concernant ou voulant les modifier. - Enfin, l'intéressé peut avoir accès à son dossier en vertu du Freedom Of Information Act en demandant à : FOIA/PA Unit, Office of Field Operations, US Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW Washington, DC 20229
Finalité du fichier	Fichier des autorités américaines Le but officiel est la sécurité. Toutefois terrorisme et grande criminalité n'ont pas été définis.
Dangers	➢ *Avis du G29 de 2007* En novembre 2007, peu de temps après la signature d'un accord entre l'union européenne et les Etats-Unis relativement à l'échange des données PNR, la Commission européenne a déposé un projet-cadre pour une nouvelle directive. Le G29, qui regroupe les autorités de protection des données personnelles européennes, a rendu un rapport sur cette décision-cadre en décembre 2007, critiquant notamment le manque de dispositions visant à assurer la sécurité des données personnelles quant à la vie privée. Il signale en particulier : « dans sa rédaction actuelle, la proposition de décision-cadre prévoit la collecte d'un grand nombre de données à caractère personnel relatives aux passagers aériens

	entrant ou sortant de l'Union Européenne, indépendamment du fait qu'ils soient soupçonnés ou innocents. Ces données seront ensuite conservées pendant une durée de 13 ans, en vue d'un éventuel usage ultérieur, permettant ainsi le profilage des voyageurs. Cette proposition s'ajoute au relevé des empreintes digitales de tous les citoyens demandant un passeport, et à la conservation de toutes les données liées au trafic des télécommunications au sein de l'UE. Un régime PNR européen ne saurait aboutir à la surveillance généralisée de tous les passagers ». Le G29 précise en outre que les Etats-Unis « n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité. Les seules informations fondées disponibles à cette fin indiquent que les données API sont davantage utilisées que les données PNR. » Ainsi, le G29 remarque qu'il ne voit pas quel besoin les Etats ont d'enregistrer, les données PNR en plus des API, d'autant que l'UE dispose déjà du Système d'Information Schengen (SIS) et prépare le système européen d'identification des visas), une base de données biométriques concernant les demandeurs de visa pour l'espace Schengen. Concernant l'échange d'informations avec les Etats tiers, le G29 s'inquiète des conséquences de la réciprocité automatique avec les pays tiers utilisant un système PNR. Selon le G29, l'existence d'un régime PNR européen pourrait inciter des régimes non démocratiques ou corrompus à exiger la communication de PNR sur la base du principe de réciprocité. Les conséquences de cette réciprocité ne semblent pas avoir été suffisamment étudiées (par exemple, en ce qui concerne la détention d'informations relatives aux cartes de crédit par un fonctionnaire d'un Etat incapable de supprimer la corruption pourrait avoir de graves conséquences). Notons également que l'acception « lutte contre le terrorisme » peut, dans certains Etats, être très différente de celle admise dans l'UE. Ainsi, la réciprocité pourrait permettre à une dictature d'établir une évaluation des risques présentés par les dissidents, à partir des données PNR. ➢ *Accord PNR Etats-Unis et Union Européenne* Après les événements du 11 septembre 2001, le Département de la Sécurité intérieure des Etats-Unis (DHS) a tenté d'avoir accès aux données PNR des Etats membres de l'Union Européenne. Le Congrès a ainsi voté deux lois exigeant ces données : « Aviation and Transportation Security Act », le 19 novembre 2001 et « Enhanced Border Security and Visa Entry Reform Act of 2002 ». En outre, Washington a négocié un accord en mai 2004 avec l'Union Européenne, l'accord PNR Etats-Unis / Union Européenne sur lequel le G29 et le parlement européen ont été très critiques. Cependant, la Cour Européenne de justice, saisie par le Parlement européen a invalidé cet accord le 31 mai 2006 dans un arrêt *Euractiv* mais uniquement sur la base légale et non sur le fond. Un nouvel accord PNR a été signé entre les Etats-Unis et l'Union Européenne, en juillet 2007. Le nouvel accord met un terme à la période d'incertitude ouverte par la décision de la Cour Européenne de justice annulant le précédent accord. Toutefois, d'après les autorités européennes de protection des données, le Parlement Européen et le contrôleur européen estiment que cet accord est loin d'offrir un niveau de protection adéquat aux données PNR transmises. Est également critiquée l'insuffisance de dispositions claires, précises et proportionnées relative au partage d'informations, de conservation, d'envois supplémentaires de données, de contrôle par les autorités de protection des données.

	Il est possible de s'inquiéter de ce que la mise en œuvre de nombreuses dispositions soit à la discrétion des Etats-Unis. ➢ En novembre 2006, l'organisation pour les libertés civiles « The Electronic Frontier Foundation » a déposé une plainte contre les « Department of Homeland Security – DHS » afin d'obtenir plus de transparence dans l'utilisation des PNR (qui sont aussi utilisés pour les vols domestiques). ➢ Risques d'espionnage et d'intelligence économique : il est ainsi possible de connaître tous les tarifs octroyés par les compagnies sur un vol et les déplacements des hommes d'affaires. ➢ Risques à l'avenir de sélection à l'entrée aux USA en fonction d'autres critères que le risque terroriste.
Législation	*En France :* Art.7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme. Elle autorise la collecte et l'exploitation des données PNR et APIS. Le ministre de l'intérieur est autorisé à créer des traitements automatisés des données à caractère personnel recueillies à l'occasion des déplacements internationaux. EN l'état aucun traitement des PNR des personnes arrivant, transitant ou partant de France n'a été mis en œuvre Art.65 du code des douanes Il permet d'exiger la communication des documents de toute nature relatifs aux opérations les intéressant. Il est possible également de requérir ponctuellement et expressément les données PNR de certains vols. Arrêté NOR/OCCO830651A du 28 janvier 2009 Ce titre crée à titre exceptionnel un traitement automatisé de données à caractère personnel relatives aux passagers, enregistrées dans les systèmes de contrôle des départs des transporteurs aériens. Résolution du Sénat n° 84 du 30 mai 2009 sur la proposition de décision cadre relative à l'utilisation des données des dossiers passagers à des fins répressives. *Union européenne* L'accès aux PNR est régulé dans l'Union européenne par différents textes relatifs à la protection des données. La directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, adoptée sans l'avis du parlement européen, se fondant sur l'accord Schengen, règle aussi les échanges de données API, dans un but officiel de lutte contre le terrorisme et contre l'immigration illégale, en autorisant « l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale » (art.12) Accord entre la commission européenne et les autorités américaines de juillet 2007 Cet accord consacre les dispositions suivantes : • Le nombre d'autorités américaines qui pourront accéder aux données PNR sur le territoire américain a été étendu ; • Les finalités d'utilisation des données PNR pourront varier en cas de modification unilatérale de leur législation par les Etats-Unis ; • La décision éventuelle de transférer des données PNR européennes vers d'autres pays tiers sera prise de manière unilatérale par les Etats-Unis, sans consultation préalable des autorités européennes ; • Il est désormais possible aux autorités américaines, « en cas de nécessité », d'avoir accès à des données dites « sensibles », c'est à dire pouvant révéler l'origine raciale, ethnique, les opinions politiques, l'état de santé des personnes, malgré un filtrage

	initialement prévu ; • Les données seront conservées 15 ans, sous forme d'une conservation « active » pendant 7 ans et « passive » pendant 8 ans, sans garantie que les fichiers non consultés soient définitivement détruits ; • Le passage du mode d'accès direct (pull) par les autorités américaines aux bases de données détenues par les compagnies aériennes au mode d'envoi des données (push) par les compagnies aériennes, ne permettant plus d'accès direct aux autorités américaines ne sera réalisé que si les conditions techniques de ce passage paraissent acceptables aux Etats-Unis ; • L'évaluation de l'application de l'accord « review » perd son caractère annuel obligatoire. Seul le commissaire européen de la Direction Générale Justice-Liberté-Sécurité sera en charge de cette inspection, sans que les autorités nationales de protection des données y soient clairement associées ; • Les autorités américaines auront la faculté de décider de manière unilatérale s'il sera répondu favorablement aux demandes des passagers européens d'accès et de rectification aux données les concernant détenues par les autorités américaines.
Campagnes de sensibilisation	Dès 2003 la LDH reprenait la communication de l'AEDH dénonçant les atteintes à la vie privée et les dangers pour la démocratie de l'accord PNR tout comme IRIS au sein du « Dialogue Transatlantique des Consommateurs (TACD) ». Lors de son congrès 2009 la LDH attirait l'attention sur les dangers de ces échanges : « Quant aux échanges de données personnelles organisés entre Etats membres de l'Union européenne (notamment par l'extension en 2007 des dispositions du traité de Prüm), voire entre l'Union et des Etats tiers (en particulier l'accord PNR passé avec les Etats-Unis en matière de données relatives aux passagers de vols transatlantiques), ils amplifient considérablement les menaces que font peser ces techniques de surveillance sur la vie privée et les libertés, en élargissant de manière très insuffisamment contrôlée le champ de diffusion des données « sensibles » collectées puis transmises, y compris par des entreprises privées. » Les jeunes comme une majorité de la population ne semblent pas sensibilisés sur ces dangers.
Recommandations	Les associations de défense des libertés et des droits de l'Homme devraient, en s'appuyant sur les avis du G29 précités et du CEDP (voir annexe EDPS-PNR), en utilisant les nouveaux pouvoirs conférés au Parlement Européen par le traité de Lisbonne, agir pour : • Que soit respecté le principe de proportionnalité et de nécessité des termes de l'accord ; • La création d'un cadre juridique sécurisé. • Obtenir un bilan des résultats concrets de l'utilisation d'un tel dispositif. • L'exclusion de toute utilisation des données sensibles relevant de la race ou de l'origine ethnique, des convictions religieuses, des opinions politiques, de l'appartenance à un syndicat, de la santé ou de l'orientation sexuelle. • Le recours au système "push" pour le transfert de données à inscrire dans ce nouvel accord (les compagnies transmettent les données à la différence du système actuel où les autorités américaines accèdent directement au fichier des systèmes de réservation aérienne. • La révision de la durée totale de conservation des données qui est disproportionnée, l'exigence d'un délai de conservation raisonnable. • Que les passagers soient informés de l'usage qui est fait de leurs données personnelles.

GEOLOCALISATION AU TRAVAIL

THEME	GEOLOCALISATION
Technologies	Il s'agit soit de l'utilisation des données relatives à l'emplacement géographique de la balise GSM à laquelle est accroché un téléphone portable soit de géo localisation par GPS (Global Positionning System) basé sur le traitement d'informations issues de satellites couplé à l'utilisation d'un réseau de communications électroniques GSM (Global System for Mobile communications).
Pays/zone d'utilisation	Europe France
Cadre d'utilisation	Selon la définition de la CNIL : « Les dispositifs dits de géolocalisation permettant aux employeurs privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation d'objets dont ils ont l'usage (badge, téléphone mobile) ou des véhicules qui leur sont confiés. »
Population concernée : cible et âge	Salariés
% d'utilisation/de la population concernée globalement et chez les jeunes	Non connu
Tendance (mesurée / supposée)	Le développement des technologies, les besoins de contrôles (qualité, sécurité etc.) laissent penser que le nombre de salariés géolocalisés est en augmentation constante.
Dangers connus / potentiels de cette technologie / Risques	la **géolocalisation d'une personne ou** d'un véhicule doit être proportionnée au but légitime recherché et que la mise sous surveillance permanente des déplacements des salariés est disproportionnée lorsque des vérifications peuvent être faites par d'autres moyens
Autres	
Les fichiers générés et leur objet	
Fichier associé et date de création	Fichier de traitement des données enregistrées. Il doit faire l'objet d'une déclaration préalable auprès de la CNIL à moins qu'un correspondant Informatique et Libertés ait été désigné au sein de l'organisme recourant à un service de géolocalisation.
Qu'est-ce qui motive l'inscription dans le fichier / Risques	Il s'agit des situations suivantes : - la sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge (travailleurs isolés, transports de fonds et de valeurs, etc.) ; - une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, (interventions d'urgence, chauffeurs de taxis, flottes de dépannage, etc.) ; - le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule (ramassage scolaire, nettoyage des accotements, déneigement routier, patrouilles de service sur le réseau routier, etc.); - le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens. En revanche, l'utilisation d'un système de géolocalisation ne saurait être justifiée lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.). La CNIL rappelle que l'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent de l'employé concerné. Ainsi que le responsable du traitement ne doit pas collecter des données relatives à la localisation d'un employé en dehors

	des horaires de travail de ce dernier. C'est pourquoi, la CNIL recommande que les employés aient la possibilité de désactiver la fonction de géolocalisation des véhicules à l'issue de leur temps de travail lorsque ces véhicules peuvent être utilisés à des fins privées. Les employés investis d'un mandat électif ou syndical ne doivent pas être l'objet d'une opération de géolocalisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat. Source : CNIL, délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.
Finalités du fichier / contenu, types de données / Risques	Les objectifs auxquels répond le dispositif peuvent être par exemple, la gestion en temps réel des interventions auprès des clients ; la lutte contre le vol. Les données collectées sont : - le nom de l'employé, - l'immatriculation du véhicule, - les kilomètres parcourus, - les temps d'arrêt, - la vitesse moyenne, - données de géolocalisation Risque de détournement de la finalité. Par exemple, l'employeur utilise le dispositif de géolocalisation pour contrôler l'activité de ses employés alors que la finalité déclarée est la lutte contre le vol. Voir : CNIL Guide de la géolocalisation des salariés - Droits et obligations en matière de géolocalisation des employés par un dispositif de suivi GSM/GPS.
Qui le détient ? Risques	L'employeur
Qui y a accès ? Partage de fichiers ? Restriction d'accès / Risques	L'accès aux données de géolocalisation doit être limité aux seules personnes qui, dans le cadre de leur fonction, peuvent légitimement en avoir connaissance au regard de la finalité du dispositif (telles que les personnes en charge de coordonner, de planifier ou de suivre les interventions, personnes en charge de la sécurité des biens transportés ou des personnes ou le responsable des ressources humaines). Le responsable du traitement doit dès lors prendre toutes précautions utiles pour préserver la sécurité de ces données et empêcher, notamment en mettant en place des mesures de contrôle et d'identification, que des employés non autorisés y aient accès. Les accès individuels aux données de géolocalisation doivent s'effectuer par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification.
Durée de conservation / Risques	1 - Les données relatives à la localisation d'un employé ne peuvent être conservées que pour une durée pertinente au regard de la finalité du traitement qui a justifié cette géolocalisation. La CNIL estime qu'une durée de conservation de deux mois paraît proportionnée. 2 - Les données de localisation peuvent être conservées pour une période supérieure à deux mois si une telle conservation est rendue nécessaire soit dans un objectif d'historique des déplacements à des fins d'optimisation des tournées, soit à des fins de preuve des interventions effectuées lorsqu'il n'est pas possible de rapporter la preuve de cette intervention par un autre moyen. Dans ces cas, la durée de conservation est d'un an 3 - Dans le cadre du suivi du temps de travail, seules les données relatives aux horaires effectués peuvent être conservées pour une durée de cinq ans.
Droit de regard ou de rectification	Le responsable du traitement doit procéder, conformément aux dispositions du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre d'un dispositif de géolocalisation des employés. Chaque employé doit pouvoir avoir accès aux données issues du dispositif de géolocalisation le concernant en s'adressant au service ou à la personne qui lui aura été préalablement indiqué.
Finalités cachées du fichier et détournement/ Risques	L'enregistrement des données de déplacement peut servir à la surveillance des salariés.
Autres	Si le salarié s'oppose à ce que les informations nominatives le concernant fassent l'objet d'un traitement, le responsable du traitement, en l'espèce l'employeur, apprécie la légitimité des

	motifs invoqués. En cas de désaccord, il appartient aux juridictions compétentes de trancher le litige.
Législation en application	
Loi / règlement / autres	Les traitements de géolocalisation, en ce qu'ils permettent de localiser l'employé utilisant le véhicule au moment où s'effectue l'opération de géolocalisation, portent sur des données à caractère personnel et sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée (article 6-2). Selon la CNIL, conformément à l'article 32 de la loi du 6/1/1978 modifiée en août 2004 et à l'article 34-1 V du Code des Postes et télécommunications électroniques, les employés doivent être informés individuellement et préalablement à la mise en œuvre du traitement : • de la finalité ou des finalités poursuivies par le traitement de la géolocalisation ; • des catégories de données de géolocalisation traitées ; • de la durée de conservation des données de géolocalisation les concernant ; • des destinataires ou catégories de destinataires des données ; • de l'existence d'un droit d'accès, de rectification et d'opposition et de leurs modalités d'exercice ; • le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un état non membre de la communauté européenne. **Il est absolument nécessaire de faire également signer chaque salarié concerné un avenant à son contrat de travail, ou d'insérer ces dispositions dans le règlement intérieur.** La géolocalisation est soumise au code du travail **(Art. L.432-2-1**) : *Préalablement à la mise en place d'un tel système, il est impératif pour l'employeur d'informer et de consulter le Comité d'entreprise ou à défaut, les Délégués du personnel sur les traitements automatisés qu'il prévoit de mettre en place, ainsi que toutes les modifications de ceux-ci.*
Risques pour les libertés malgré l'encadrement par la loi	Surveillance abusive du salarié par l'employeur, atteinte à la vie privée.
Autre	Par une délibération du 17 novembre 2005, la CNIL s'est opposée à un projet de personnalisation des primes d'assurance en fonction de l'usage réel d'un véhicule. En l'espèce, l'assureur proposait de réduire le montant de la prime en contrepartie de l'installation d'un système de géolocalisation à bord du véhicule afin de lui permettre de vérifier le cas échéant le respect des engagements contractuels. La géolocalisation devait permettre en particulier de contrôler le respect des vitesses maximales autorisées. La CNIL s'y est opposée et a rappelé plusieurs principes issus de la loi du 6 janvier 1978 modifiée. Tout d'abord, l'article 9 de cette loi ne permet pas à une personne de droit privé de mettre en œuvre un traitement relatif aux violations des limitations de vitesse. Un assureur ne peut donc pas enregistrer les excès de vitesse de ses clients.
Si révision de la réglementation : raison / résultats : amélioration ou aggravation	Nécessité d'avoir une analyse plus détaillée des usages actuels et futurs afin d'évaluer les restrictions à imposer. Une réglementation spécifique permettrait de réduire les risques d'atteintes à la vie privée et aux libertés.
Conformité avec le droit européen	Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Directive 2002/58/CE du 12 juillet 2002 complémentaire concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
Application ou non de la législation / Risques	

Autres	Avis de mai 2008 du « Groupe 29 » sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée. avis de 2005 : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_fr.pdf
Ces outils et le public jeunes et jeunes adultes	
Niveau auquel ils sont concernés ou importance de l'utilisation	Non connu
Conscience des problèmes ou des risques encourus	Non connu
Indifférence ou réaction	En 2008, 70 plaintes reçues par la CNIL sur des problèmes d'utilisation de la géo localisation pour contrôler les horaires de salariés.
Campagnes de sensibilisation / impact	Néant
Bonnes pratiques	Recommander que les employés puissent désactiver la fonction de géolocalisation des véhicules à l'issue de leur temps de travail lorsque ces véhicules peuvent être utilisés à des fins privées.
Campagnes à mener / Sur quels aspects	Faire connaitre leurs droits aux salariés à travers les syndicats et les CE qui doivent être consultés : Information préalable, limites de la surveillance
Conclusions	
Recommandations	Dans la mesure où ces pratiques concernent essentiellement des salariés, les associations devraient mener des campagnes de sensibilisation vis-à-vis des syndicats pour l'application de la législation et notamment pour - le respect du principe de finalité dans chacun des traitements effectués - l'information des salariés concernés sur leurs droits, - l'anonymisation systématique des données,

GEOLOCALISATION PAR TELEPHONE PORTABLE

THEME	GEOLOCALISATION PAR TELEPHONE PORTABLE
La technologie utilisée	• Système GPS (Global Positionning System). • Système GSM (Global System for Mobile communications). • Personal Digital Assistant, assistant numérique personnel Wi-Fi. • Adresse IP des ordinateurs.
Pays/zone d'utilisation	France (Europe monde)
Utilisation	• Localisation des employés et/ou des véhicules d'une entreprise (voir fiche précédente). • Localisations de personnes (notamment des enfants ou des personnes âgées) et/ou d'objets pour les particuliers. • Utilisations pour des fins commerciales : fournitures de services ou de publicités correspondant à la zone où la personne se trouve. Le Système GPS permet d'obtenir la position d'une personne ou d'un objet à tout moment. Il s'appuie sur un réseau de satellites, il peut retransmettre cette information à un système centralisé. Le Système GSM (Global System for Mobile communications) est la norme numérique pour la téléphonie mobile. Il s'appuie sur la couverture du territoire par des antennes terrestres. Selon la densité de la population ou le relief, leur nombre sera plus ou moins important. Avec la norme UMTS (Universal Mode Mobile Télécommunications) on peut passer du système terrestre au système satellitaire. (Iphone par exemple, avec la technologie 3G incorporée). La localisation est très rapide, moins de 5 secondes, mais la précision aléatoire, 100 à 700 mètres en zone urbaine, près de 10 kilomètres en zone rurale. Les PDA sont également de plus en plus utilisés pour des usages de géolocalisation, de cartographie et de navigation routière lorsqu'ils sont couplés à un dispositif de géolocalisation (**GPS**, *Global Positionning System*). En effet, pour un faible coût il est possible de disposer d'un système GPS embarqué très performant permettant une navigation routière à l'aide d'une carte indiquant en permanence sa position, la vitesse et une représentation visuelle de la route (éventuellement en 3D) avec des instructions à l'écran et dictées par une voix de synthèse. Des logiciels permettent de localiser les adresses IP : http://www.geolocalise-ip.com/ ou localisation par Localité,longitude-latitude : http://www.maxmind.com/app/lookup_city
Statistiques concernant la population	Toutes les tranches d'âge. Il existe cependant un système de géolocalisation particulièrement dédié aux enfants : Ce service s'appelle OOTAY de la société Illico.net, c'est un service de géolocalisation des enfants via leur téléphone mobile Orange ou Bouygues télécom. Ce système de «géo contrôle parental» repose sur un principe simple : l'adulte s'inscrit au service en ligne et y enregistre les noms et coordonnées téléphoniques de son enfant. Pour le localiser, il accède ensuite à son espace dédié sécurisé (identifiant et mot de passe), via le Net ou sur un mobile compatible Wap ou iMode. En cliquant sur le nom de l'enfant, une requête est envoyée sur le réseau mobile d'Orange pour repérer le téléphone. En réponse, le parent reçoit une carte indiquant le périmètre géographique où se situe le mobile. Ce périmètre est représenté par un cercle de couleur. Le service fonctionne sur toute la France avec une précision de 50 à 150 mètres en ville, et de 150 mètres à 3 kilomètres en zone rurale.

	La Commission nationale de l'informatique et des libertés (Cnil) a validé le dossier d'Illico.net. Il existe d'autres services de géolocalisation au service des particuliers : Google latitude maintenant disponible sur iPhone, Google Maps sur les ordinateurs.
Fichiers générés	Fichiers des opérateurs de téléphonie
Contenu	Données de gestion de l'abonné + données de géolocalisation
Durée de conservation	Pour les opérateurs de télécommunication, en France la durée de conservation des géolocalisations (position de la balise à laquelle un téléphone portable est accroché au moment de l'émission et de la réception d'un appel) est d'une année.
Qui détient ces données ? **Qui y a accès ?**	L'opérateur, le fournisseur de services,
Droit de regard et rectification	l'opérateur doit obtenir l'autorisation préalable de l'abonné pour enregistrer et stocker les données. En plus de cette autorisation l'opérateur doit fournir à son client un moyen technique simple de s'opposer à tout moment, à l'occasion de n'importe quelle connexion, à l'enregistrement de sa géolocalisation. L'opérateur doit donner au préalable à son client une information claire et complète sur les conditions d'utilisation de ces données (transmission ou non à des tiers, durée de conservation etc.).
Finalité du fichier	
Dangers	La géolocalisation peut donner lieu à de nombreux abus et nuire à la vie privée et à la liberté d'aller et venir. En général, l'opérateur utilise l'opt-in, l'utilisateur doit s'inscrire au service et donner son accord à chaque géolocalisation ou en être averti. Il doit aussi pouvoir revenir sur sa décision simplement et gratuitement. L'inverse de l'opt-in, l'opt-out ne requiert pas l'approbation de l'utilisateur.
Autres	Présentée comme un confort, la géolocalisation est en passe de devenir une application universelle qui s'insinue dans notre quotidien et le suivi de nos déplacements tend à devenir une contrainte acceptée. Les dangers potentiels sont nombreux : Atteintes à la vie privée. Atteintes aux libertés. Atteinte à la liberté de circuler anonymement.
Législation	
	Les données de géolocalisation transmises par un téléphone portable à l'opérateur, ensuite utilisées et stockées par ce dernier, se définissent en droit français et européen comme des " données à caractère personnel " puisqu'elles donnent des informations sur une personne physique que l'on peut identifier. Elles sont donc soumises, pour leur collecte, leur utilisation et leur conservation, à la loi française " informatique et libertés " de 1978 modifié par la loi du 4 août 2004. La Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques qui soument la géolocalisation au consentement préalable de l'utilisateur du portable. Recommandations de la CNIL et du G29 sur les services de géolocalisation dans le contexte des relations de travail et des services visant les enfants Par une délibération du 17 novembre 2005, la CNIL s'est opposée à un projet de personnalisation des primes d'assurance en fonction de l'usage réel d'un véhicule. En l'espèce, l'assureur proposait de réduire le montant de la prime en contrepartie de

	l'installation d'un système de géolocalisation à bord du véhicule afin de lui permettre de vérifier le cas échéant le respect des engagements contractuels. La géolocalisation devait permettre en particulier de contrôler le respect des vitesses maximales autorisées. La CNIL s'y est opposée et a rappelé plusieurs principes issus de la loi du 6 janvier 1978 modifiée. Tout d'abord, l'article 9 de cette loi ne permet pas à une personne de droit privé de mettre en œuvre un traitement relatif aux violations des limitations de vitesse. Un assureur ne peut donc pas enregistrer les excès de vitesse de ses clients.
Autre	
Campagnes	Campagnes d'information et de sensibilisation sur les implications en matière d'atteintes aux libertés de l'utilisation de la géolocalisation. Informations à diffuser sur l'interdiction de la géoocalisation sans le consentement préalable de la personne concernée.
Recommandations	Exiger des opérateurs l'application de la législation en matière d'autorisation préalable et par ailleurs que les conditions générales d'utilisation soient suffisamment explicites. Alerter les autorités de protection de la vie privée (+ défenseur des enfants) sur la multiplication des outils de surveillance parents/enfants / personnes âgées qui seraient mis en œuvre de manière abusive

Identité biologique

PASSEPORT BIOMETRIQUE

THEME	PASSEPORT BIOMETRIQUE
Le recensement des technologies	Radio frequency identification, biométrie et base de données
Technologies utilisées	Utilisation de trois technologies : 1) RADIO FREQUENCY IDENTIFICATION - RFID (voir fiche passe Navigo) Selon Gemalto la société fabricant les puces : « Les informations contenues dans la puce et appartenant aux groupes de données obligatoires 1 et 2 (zone lisible par un lecteur optique et image faciale du passeport) confirment effectivement les informations imprimées. Néanmoins, l'image faciale enregistrée dans la puce est d'une résolution supérieure à la photographie imprimée : lorsqu'elle est visualisée sur l'écran du contrôle de police, elle permet une identification plus sûre de la personne. » 2) Données biométriques : La biométrie est une technique visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Les deux techniques biométriques utilisées ici sont : les empreintes digitales (huit empreintes dans la base de données et deux dans la puce RFID) et la photographie du visage numérisée. Les empreintes digitales (finger-scan) : la donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme. L'identité des emplacements de plus de 14 minuties (croisement de deux sillons ou de deux crêtes) entre deux empreintes est considéré comme suffisant pour dire que ces deux empreintes appartiennent à la même personne 3) Création de bases de données.
Pays	France
Cadre d'utilisation	Document officiel servant à prouver son identité exigé pour les déplacements vers les pays étrangers (hors U.E).
Population concernée	L'ensemble de la population de nationalité française est concerné sans distinction d'âge. Seuls les enfants de moins de 6 ans ne sont pas soumis au relevé d'empreintes digitales.
Dangers connus	La RFID induit un risque de traçage et de profilage des personnes. Accusées de porter atteinte à la vie privée des citoyens. (Voir fiche Passe Navigo). Contenu de la puce du passeport : la photo d'identité numérisée, les empreintes digitalisées de deux doigts ainsi que toutes les données d'état civil inscrites sur la première page du passeport lui-même. Tout autre lecteur de puce qui recevrait un signal de celle-ci pourrait récupérer les informations biométriques sans même que l'intéressé ne s'en aperçoive Les données biométriques contenues dans la puce et dans la base de données empreintes digitales, sont une donnée biométrique qui peut d'une part être altérée (accidents, travail avec des produits chimiques etc.) ; d'autre part les traces d'empreintes digitales laissées sur différents supports (poignées de portes, vitres etc.) peuvent être relevées à l'insu de la personne et reproduites. Par ailleurs le nombre de points distinctifs (les minuties) relevés n'est pas suffisant pour éviter les fausses reconnaissances et les faux rejets lors des validations par lecture de la puce RFID et scan de l'empreinte de son porteur. La constitution de base de données peut permettre de caractériser très facilement une partie d'une population (risque de discriminations) voir recours La biométrie n'est pas une "solution miracle et universelle".
Fichier généré	Création d'un système de traitement automatisé de données à caractère personnel (fichier central dénommé TES), première base centralisée de données biométriques à finalité administrative

	portant sur des ressortissants français, comportant les photographies des demandeurs de passeport et les empreintes digitales de huit doigts, ce qui va au-delà de ce qui est prévu par la législation européenne. (Avis de la Cnil visible en annexe.)
Qu'est ce qui motive l'inscription dans le fichier ?	Toute demande de passeport pour les ressortissants français
Finalité du fichier/ contenu, types de données/ Risques ?	Mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports, ainsi que pour prévenir, détecter et réprimer leur falsification et leur contrefaçon. Les données à caractère personnel enregistrées dans le système de traitement automatisé sont : a) Les données relatives au titulaire du passeport : - le nom de famille, les prénoms et, si le requérant le demande, le nom dont l'usage est autorisé par la loi, la date et le lieu de naissance, le sexe ; - la couleur des yeux, la taille ; - le domicile ou la résidence ou, le cas échéant, la commune de rattachement de l'intéressé ou l'adresse de l'organisme d'accueil auprès duquel il est domicilié ; - le cas échéant la décision attestant la capacité juridique du demandeur ; b) – les empreintes digitales de huit doigts. c) – Une photographie numérisée. d) Les informations relatives au titre : - numéro de demande et de série fiscale du passeport ; - type de passeport ; - tarif du droit de timbre ; - date et lieu de délivrance ; - autorité de délivrance ; - date d'expiration ; - mention, avec la date, de la perte, du vol, de la destruction, de l'annulation ou du retrait ; - mentions des justificatifs présentés à l'appui de la demande de passeport ; - informations à caractère technique relatives à l'établissement du titre ; - informations relatives à la demande de passeport : numéro de demande, lieu de dépôt, date de réception de la demande, date de l'envoi du titre au guichet de dépôt, motif de non-délivrance ; c) Les données relatives au fabricant du passeport et aux agents chargés de la délivrance du passeport : - identifiant de l'agent qui enregistre la demande de passeport ; - identifiant du fabricant du passeport ; - références des agents mentionnés à l'article 20 du Décret n° 2005-1726 (voir § loi).
Qui le détient / Risques	Le ministère de l'intérieur
Qui y a accès / Partage de fichier / Restrictions d'accès / Risques	Accès : Les destinataires des données à caractère personnel enregistrées dans le système de traitement automatisé prévu à l'article 18 et dans le composant électronique prévu à l'article 2, sont les fonctionnaires du ministère de l'intérieur spécialement affectés dans le service mettant en œuvre ledit système, ainsi que les seuls agents et personnels spécialement affectés à l'instruction des demandes de délivrance des passeports, énumérés ci-après : - les agents chargés de l'application de la réglementation relative au passeport au ministère de l'intérieur et au ministère des affaires étrangères, individuellement habilités par le ministre de l'intérieur ou le ministre des affaires étrangères ou par les fonctionnaires que ces ministres ont désignés à cet effet ; - les agents des préfectures et des sous-préfectures chargées de la délivrance des titres visés aux articles 4 et 15, individuellement habilités par le préfet ou le sous-préfet ; - les agents diplomatiques et consulaires chargés de la délivrance des titres visés aux articles 4 et 15, individuellement habilités par l'ambassadeur ou le consul ; - les agents chargés de la délivrance des passeports de service au ministère de l'intérieur, individuellement habilités par le ministre de l'intérieur ou par les fonctionnaires désignés par le

	ministre à cet effet. Pour les besoins exclusifs de l'accomplissement de leurs missions, les personnels chargés des missions de recherche et de contrôle de l'identité des personnes, de vérification de la validité et de l'authenticité des passeports au sein des services de la police nationale, de la gendarmerie nationale et des douanes peuvent accéder aux données à caractère personnel contenues dans le composant électronique du passeport prévu à l'article 2 et enregistrées dans le système de traitement automatisé prévu à l'article 18. Risques : La procédure d'habilitation spéciale et individuelle des agents qui auront accès aux données enregistrées dans le fichier est-elle suffisamment stricte pour que d'autres agents n'y aient pas accès ? Autre risque: Il n'est pas prévu de vérifier l'authenticité des documents requis pour établir le passeport biométrique (copie intégrale de l'acte de naissance, etc .) ce qui ne le rend plus efficace contre l'usurpation d'identité. Interconnexions : Le système de traitement automatisé prévu à l'article 18 du Décret n° 2005-1726 (voir § loi) fait l'objet d'une interconnexion avec les systèmes d'information Schengen et INTERPOL. Cette interconnexion porte sur les informations relatives aux numéros des passeports perdus ou volés ainsi que sur l'indication relative au pays émetteur, au type et au caractère vierge ou personnalisé du document. Risque d'interconnexions à terme avec d'autres fichiers et notamment d'autres fichiers contenant des données biométriques.
Durée de conservation	La durée de conservation des données à caractère personnel enregistrées dans le système de traitement automatisé prévu à l'article 18 est de quinze ans lorsque le titre est délivré à un majeur et de dix ans lorsqu'il est délivré à un mineur. En prenant en considération les renouvellements de passeports on peut donc considérer que la durée de conservation des données est à partir de la première demande d'un passeport celle de toute la durée de la vie de son porteur
Droit de regard ou de rectification	La remise du passeport s'accompagne d'une copie sur papier des données nominatives enregistrées dans le composant électronique. Le titulaire exerce son droit de rectification pour ces données auprès de l'autorité de délivrance. Le droit d'accès et le droit de rectification s'exercent auprès de l'autorité de délivrance dans les conditions fixées aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée en 2004.
Finalité cachée du fichier et détournements/ Risques	Constitution d'une base de données centralisée des empreintes digitales et des photos numériques de l'ensemble des Français… dans l'attente de la carte d'identité biométrique obligatoire.
Législation en application	
Loi	Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques. Voir annexe Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques. Voir annexe En 2008, la Ligue des droits de l'Homme a déposé une requête devant le Conseil d'Etat tendant à l'annulation du décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports biométriques, ce décret violant le principe de proportionnalité prévu à l'article 6, 3° de la loi du 6 janvier 1978. Voir annexe L'examen de la requête est toujours en cours.
Conformité avec le droit européen	La prise des empreintes digitales de huit doigts va au-delà de ce qui est prévu par la législation européenne, et certains états membres de l'Union Européenne (Allemagne par exemple) ont mis en œuvre des passeports biométriques sans pour autant créer des bases centrales d'empreintes digitales. Le Contrôleur européen de la protection des données dans son avis du 26 mars 2008 recommande "à la Commission de proposer de nouvelles mesures d'harmonisation afin que les données biométriques collectées pour être intégrées dans les passeports délivrés par États membres de l'UE ne puissent être stockées que sur un support décentralisé (sur la puce RFID du

	passeport)" L'apparition de nouvelles finalités au traitement prévu par le règlement communautaire n°2252/2004. Le ministère de l'Intérieur est en effet autorisé à procéder à la création de la base centralisée dénommée TES pour prévenir et détecter la falsification et la contrefaçon des passeports (article 7 du décret du 30 avril 2008), et non plus seulement à l'établissement, la délivrance, le renouvellement et le retrait des passeports. Voir le texte de la requête précitée
Ces outils et le public jeunes et jeunes adultes	
Niveau auquel ils sont concernés ou importance de l'utilisation	Les adolescents et les jeunes adultes sont concernés comme l'ensemble de la population dans la mesure où ils demandent l'obtention d'un passeport.
Conclusions	
Recommandations	Les associations de défense des droits et libertés devraient mobiliser les citoyens et les élus pour obtenir que : • Les données biométriques collectées pour être intégrées dans les passeports ne soient stockées que sur la puce RFID du passeport (comme en Allemagne) (voir CEPD). Ce qui impliquerait que la base de données TES ne pourrait plus être utilisée comme une base de données policière et de fichage ethno-racial. • Le gouvernement s'attaque à la sécurisation du processus d'obtention car le principal vecteur de la fraude en matière de papier d'identité est la production de fausses pièces justificatives, l'acte d'état civil devrait pouvoir être dématérialisé pour être transmis directement de l'administration détentrice (mairies) à l'administration émettrice du passeport biométrique. • Des garanties soient données sur les habilitations des personnes ayant accès à la base de données et sur le contrôle de ces accès. Par ailleurs elles doivent alerter sur le fait que le rapport des individus à l'Etat est modifié par l'utilisation de la biométrie : il n'est plus basé sur l'identité déclarative (né le :… à :… fils de :… etc.) mais sur le corps de l'individu.

CONTROLE ETABLISSEMENTS SCOLAIRES ET DES ENTREPRISES

THEME	BIOMETRIE
Technologie utilisée	Lecteur d'empreintes digitales ou palmaires : 1) **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. 2) **Empreintes palmaires :** cela consiste à capturer une image en 3D de la main et d'en extraire plusieurs dizaines de points prenant en compte la largeur, la longueur, la forme des doigts, etc.
Pays	France
cadre d'utilisation	Accès aux écoles et/ou restaurants scolaires. Accès aux entreprises et/ou aux restaurants d'entreprises. Même si cela concerne principalement les restaurants scolaires et les 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 relative 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	Adultes salariés de certaines entreprises. Jeunes à partir de l'âge de six ans. Avant cet âge, les différentes empreintes ne sont pas fixées.
Durée de conservation	Elles sont variables 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 salariés dans les entreprises avec les droits d'accès Les fichiers des élèves dans les établissements scolaires
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[5] 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 :* En ce qui concerne la biométrie à l'école, le principal d'un collège équipé de ce dispositif déclare : 1) « Les parents l'ont approuvé à l'unanimité.» 2) « Les demi-pensionnaires trouvent plutôt rigolo ce moyen de reconnaissance par la main. » Ce système est présenté comme un confort, une commodité et un facteur d'économie : plus de perte de cartes de cantine ou de bibliothèque. Toutefois 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. Louis Joinet, ancien directeur de la Commission Nationale de l'Informatique et des Libertés (Cnil), et 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*

[5] Groupement des industries de l'interconnexion des composants et des sous ensembles électroniques

	un instrument de contrôle, comme si c'étaient des bêtes. » Des parents d'élèves, des syndicats (de l'Education nationale ex : FSU, de magistrats) 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 34*)*. 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 G29pour : Alerter l'ensemble de la population, les parlementaires nationaux et les institutions européennes sur les dangers à utiliser la biométrie pour l'identification des personnes. Dénoncer les intérêts financiers des industriels qui rejoignent les intérêts politiques de contrôle des citoyens.

Communications Interpersonnelles

MESSAGERIE G MAIL

THEME	**COMMUNICATIONS INTERPERSONNELLES :** **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	Pays : France/monde. Courrier électronique (courriel) échange de textes, fichiers joints (textes, sons, images) entre différents interlocuteurs (particuliers / particuliers, entreprises, 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) ; Offre aussi une option de messagerie instantanée (chat). 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 : les nom, prénom, nom choisi pour l'adresse mail 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 l'inscription dans le fichier ? Améliorer la qualité des services. Google annonce utiliser 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. Le service Gmail comprend des annonces pertinentes et des liens connexes sur la base de l'adresse IP, du contenu des messages et d'autres informations relatives à notre utilisation de Gmail. Les ordinateurs de Google traitent les informations contenues dans nos messages à des fins diverses notamment pour la mise en forme et l'affichage des informations, 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. Tout comme les autres services web, 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	Au départ Google entendait conserver les informations sur les recherches effectuées sur son moteur de recherche 2 ans puis 18 mois. La durée de conservation a finalement été réduite 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 votre pays de résidence. Cela implique que pour Google, la législation qui s'applique est celle est USA. Google ainsi que les tiers que Google autorise peuvent avoir accès à ces données. Ainsi, dans les conditions générales de Google, on peut lire : « Lorsque nous faisons appel à des tiers pour nous assister dans le traitement de vos informations personnelles, nous veillons à ce que ces derniers respectent nos règles de confidentialité et toutes autres mesures de confidentialité et de sécurité appropriées. Nous sommes également susceptibles de communiquer certaines informations à des tiers dans des cas limités, notamment en cas de recours légal, de prévention des fraudes, de

protection face à un risque imminent et pour préserver la sécurité de notre réseau et de nos services. »

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

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.

Concernant la sécurité des informations :

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 pour la création du compte. Extrait des conditions de l' « Avis de confidentialité de Gmail » : « Vous pouvez résilier votre compte via la section *Compte Google* des paramètres Gmail. De telles suppressions ou résiliations prendront effet immédiatement dans l'affichage de votre compte. Les copies résiduelles des messages et comptes supprimés seront effacées de nos serveurs actifs au plus tard 60 jours après leur suppression et pourront être conservées sur nos systèmes de sauvegarde hors ligne ». 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 ».
Dangers	• **Sollicitations marketing** • **Spams,** • **Phishing = "hameçonnage" ou "filoutage"** • **Piratage des données :** - En octobre 2008 un chercheur a démontré qu'il pouvait intercepter le contenu d'une session avec une application web, par exemple Gmail (ou Facebook), il pouvait par exemple 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. En effet le système de connexion sécurisée (lorsque « https » est affiché dans la barre de navigation) par défaut, n'est actif que pour la saisie des identifiants, ensuite la connexion n'est plus sécurisée. L'option permettant la connexion en mode sécurisé est désactivée par défaut et 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	<u>Concernant les Messageries en général</u> 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. En outre, 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 : a) Puisque rien n'y oblige ne pas déclarer sa véritable identité lors de l'ouverture d'un compte Gmail b) Utiliser un anti-virus et un anti-spam c) 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 mail 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) d) Utiliser une adresse e-mail spécifique pour les services en ligne sur internet et une autre pour les échanges avec famille, amis et autres. e) Changer l'adresse e-mail (spécifique) si elle reçoit trop de spams f) Ne jamais répondre aux spams y compris pour protester, ceci révèlerait la validité de l'adresse g) Lire les conditions générales d'utilisation. Lors de la création du compte et la saisie d'un mot de passe, Gmail propose d'indiquer une réponse à une question pour s'identifier en cas de perte de mot de passe. Dans la liste, 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 !). Si on veut éviter le "profilage total" utiliser une autre solution de messagerie gratuite surtout si l'on utilise fréquemment le moteur de recherche de Google. 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
Autres	Le gouvernement à travers le « Secrétariat général de la Défense Nationale » et « l'Agence nationale de la sécurité des systèmes d'information » publie des conseils et des informations techniques très détaillées sur la sécurité sur internet. Les internautes gagneraient sans doute à connaître ce site. **http://www.securite-informatique.gouv. fr/gp_article74.html**
Recommandations	Insister auprès des pouvoirs publics (nationaux et européens) et des autorités de protections des données personnelles pour que Google soit soumis au droit européen.

MESSAGERIE FAI (OU FSI)[6]

THEME	COMMUNICATIONS INTERPERSONNELLES : Messagerie FAI (exemple : SFR)
La technologie utilisée	Un fournisseur d'accès Internet est un organisme, généralement une entreprise, offrant une connexion au réseau informatique Internet. Utilisation : Connexion internet - réseau - modem bas ou haut débit – wifi. Les possibilités : courrier électronique (courriel) échange de textes, fichiers joints (textes, sons, images) entre différents interlocuteurs (particuliers ➔ particuliers, entreprises, administrations etc.). Protocoles d'envoi des courriers électroniques utilisés : SMTP (Simple Mail Transfer Protocol, Protocole Simple de Transfert de Courrier). La technologie : Protocole de réception des courriers électroniques : POP et IMAP Le protocole POP (Post Office Protocol) permet de récupérer le courrier sur un serveur e-mail. Le protocole IMAP (Internet Message Access Protocol) est un protocole qui à chaque connexion synchronise le contenu de la boite e-mail sur le serveur vers le logiciel de messagerie. (L'IMAP permet donc contrairement au POP de se connecter et lire ses e-mails sur différents ordinateurs ou/et téléphone mobile et de retrouver tous les dossiers et e-mails archivés). L'expéditeur est identifié par son adresse de messagerie, idem pour les destinataires. Il est possible d'avoir accès à ce fournisseur d'ordinateurs personnels, ou dans des lieux privés ou publics tels que des établissements scolaires, universitaires ou alors des cybercafés, dans des entreprises, à partir d'ordinateurs portables dans les lieux équipés de WIFI ou à partir de téléphones portables types smart phones.
Pays d'utilisation	France/monde
Législation	• Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés • Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique • Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance • Loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs • Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie • Loi d'orientation et de programmation pour la sécurité intérieure (LOPSI) : • Le nouvel article 222-16-1 du code pénal réprime l'utilisation malveillante, dans le cadre des communications électroniques, de l'identité d'autrui ou de toute autre donnée personnelle, en vue de troubler sa tranquillité ou de porter atteinte à son honneur ou à sa considération. Il sanctionne ces comportements, sur le modèle des appels téléphoniques malveillants, d'une peine d'un an d'emprisonnement et de 15 000 € d'amende. Conformité avec le droit européen : • Directive relative à la protection des données 95/46/CE • Directive E-Privacy de 1997
Statistiques concernant la population	Selon l'Observatoire des usages Internet du cabinet d'analyse **Médiamétrie** : en 2009, 25,9 millions de Français utilisent régulièrement la messagerie électronique. SFR compte 3,8 millions d'abonnés fin 2008. Autre source : Près de 32 millions d'internautes en France en juillet 2008

[6] FAI : Fournisseur d'Accès Internet, FSI : Fournisseur de Services Internet

	(http://www.journaldunet.com/cc/01_internautes/inter_nbr_fr.shtml) Toujours selon Médiamétrie, les jeunes de18 à 24 ans représenteraient 1/5 des internautes (internet en général – pas de chiffres pour les messageries). En **1999** : 3 millions d'internautes Français âgés de plus de 18 ans. En **2009** : 29 millions.
Fichiers générés **Fichiers associés**	• Fichier de gestion commerciale constitué par une entreprise privée, enregistrement des données d'inscription du client. • Fichier des données de communications électroniques à conserver obligatoirement par les fournisseurs d'accès internet (FAI).
Durée de conservation	Notons que les FAI doivent conserver pendant un an les données de connexion de leurs clients, soit : • Les informations permettant d'identifier l'utilisateur, • données relatives aux terminaux de connexion utilisés • caractéristiques techniques ainsi que date, horaire de communication • données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs • les données permettant d'identifier le ou les destinataires de la communication (en-tête des messages, adresses mail des destinataires, objet) Aucune indication sur la destruction de celles-ci au terme de la durée de conservation ni sur le chiffrement de ces données.
Qui détient les données ? **Qui y a accès ?**	Le nombre de personnes ayant accès à ces données n'est pas connu. Le fournisseur d'accès internet y a accès.
Droit de regard et rectification	La loi informatique et libertés le prévoit. Exemple : Conditions générales d'utilisation SFR **Condamnations :** Exemple : La CNIL vient d'annoncer une sanction de 7000 euro prononcée le 12 juin 2008 à l'encontre de Neuf-Ci, anciennement Club Internet. (CNIL, délibération n° 2008-163, 12 juin 2008) Une abonnée de Club Internet avait demandé l'accès à l'ensemble des données la concernant détenues par l'opérateur. Après un refus, elle avait enfin reçu quelques informations (nom, adresse, références bancaires), mais rien de plus (éléments enregistrés lors de ses appels notamment). Comme la loi l'y autorise, cette cliente avait saisi la CNIL. Suite à plusieurs demandes sans réponse, celle-ci avait adressé au fournisseur d'accès une mise en demeure sous un délai d'un mois. Club Internet avait annoncé la mise en place de chartes de données personnelles, un an plus tard, les chartes de données personnelles étaient toujours à l'état de projet. Quant à la mise en demeure, la CNIL n'a reçu que de maigres éléments de réponse. C'est suite à ces éléments qu'a été prononcée le 12 juin 2008 cette sanction de 7000 euro à l'encontre de Neuf-CI.
Dangers	• Spams, • Solicitations marketing • Phishing (hameçonnage), • Usurpation d'identité • La rétention des données de connexion par le FAI dans le cadre de la lutte contre le terrorisme • Notons que l'utilisation de la messagerie d'entreprise à des fins privées, peut faire courir le risque de contestation du statut de « correspondance privée ». • L'Article 1 de la loi N° 91-646 du 10 juillet 1991 garantit le secret des correspondances émises par la voie des télécommunications, la violation du secret tombant sous le coup de l'art 226-15 du code pénal. Toutefois

	l'employeur doit pouvoir accéder aux moyens mis à disposition du salarié et donc à la messagerie utilisée. • Divulgation de données personnelles aux autorités judiciaires, tout internaute étant un suspect en puissance. Conscience des dangers : 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. Notons que seulement 20 % de ces jeunes 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.
Communication	Campagnes menées : Il existe des campagnes pour les plus jeunes sur les dangers de l'internet en général, initiées par la CNIL, l'Education nationale, le forum des droits de l'Internet : le guide pratique « Internet et moi » a été réalisé par le Forum des droits sur l'internet et Okapi (journal pour enfants) avec le soutien du Collectif Inter associatif Enfance et Media (CIEM), de la Délégation Interministérielle à la Famille et de Microsoft. Le guide délivre une foule de conseils sur les principaux usages que font les ados de l'internet et propose un quiz en 10 questions. Le guide « Internet et moi » est conforme à l'état du droit au jour de sa publication (25 avril 2007). Un Collectif **" L'Internet plus sûr, on se mobilise ! "** composé notamment de Microsoft et d'autres sociétés privées ainsi que des agences du gouvernement dédiées à l'internet a lancé une campagne pour la protection de la vie privée. Sur le site http://www.protegetonordi.com/ on trouve de nombreux conseils, des jeux, des BD à destination de différents publics : enfants, ados, parents enseignants. L'impact de ces campagnes est cependant inconnu. Campagnes à mener : • Lutte contre les spams, contre l'utilisation des données pour des campagnes marketing, contre le phishing (filoutage). • Inciter les utilisateurs à lire des CGU et exiger que celles-ci soient accessibles à tous (compréhensibles par tous). Campagnes de revendications : Exiger de connaitre le traitement des fichiers de rétention des données *Les bonnes pratiques* • 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 des "amis" sur internet. • Ne pas publier son adresse mail sur internet • Utiliser une adresse e-mail spécifique pour les services en ligne sur internet et une autre pour les échanges avec famille et amis. • Changer l'adresse e-mail (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 du FAI
Autres	La société américaine « Rampell Software » propose, depuis la fin du mois de mai 2004, un nouveau service de suivi du courrier électronique intitulé « Did they read it ?» (en français « L'ont-ils lu ? »). Ce service permet à un internaute, moyennant le paiement d'un

	abonnement, de savoir : la date et l'heure d'ouverture de l'e-mail ; la position géographique de la personne qui l'a ouvert ; combien de fois et pendant combien de temps ; si la personne a transmis l'e-mail à d'autres personnes et depuis quel serveur de messagerie. Il permet également de connaître le navigateur utilisé par le destinataire ainsi que son système d'exploitation. Le processus se déroule entièrement à l'insu des destinataires des messages électroniques. A la différence des services d'accusé de réception fournis par les logiciels de messagerie « classiques », le destinataire n'a pas le choix d'accepter ou de refuser de retourner les informations à l'abonné à « Did they read it ?». Il n'en est même pas informé. Par principe, la CNIL ne peut qu'émettre les plus vives réserves sur un tel procédé. En effet il s'agit d'une collecte d'informations nominatives car sont ainsi enregistrées et transmises des informations détaillées sur le « comportement » du destinataire d'un message électronique. Une telle collecte, effectuée à l'insu des personnes, est contraire aux règles de protection des données et plus précisément à l'article 25 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui interdit la collecte de données nominatives opérée par tout moyen frauduleux, déloyal ou illicite. La CNIL rappelle que le non-respect de ces dispositions est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-18 du code pénal). En conséquence, la CNIL attire l'attention des entreprises françaises, des administrations et plus largement du public sur le fait qu'en s'abonnant à « Did they read it ?», toute personne basée sur le sol français est susceptible d'encourir des poursuites pénales.
Recommandations	

TWITTER

THEME	RESEAUX SOCIAUX / Communications interpersonnelles
La technologie utilisée **Contenu du fichier**	**TWITTER :** il s'agit d'un outil de réseau social et de microblogging qui permet à l'utilisateur d'envoyer gratuitement de courts messages (140 caractères maximum, soit 1 ou 2 phrases) appelés « tweets » (gazouillis) par internet, messagerie instantanée ou par SMS. Twitter a été créé à San Francisco au sein de la start-up Odeo-Inc fondée par Noah Glass et Evan Williams. Odeo proposait une plate-forme d'hébergement, de diffusion et d'enregistrement de podcasts. L'idée de départ était de permettre aux utilisateurs de décrire ce qu'ils étaient en train de faire via SMS. Ouverte au public le 13 juillet 2006, la première version s'intitulait Stat.us puis twittr en référence au site de partage de photos Flickr puis twitter son nom actuel. Contrairement à un blog normal, Twitter n'invite pas les lecteurs à commenter les messages postés. Le slogan initial était : « What are you doing ? ». Cela permettait de raconter ce que l'on faisait au moment où on le faisait. Twitter le remplace par « What's happening » avec une possibilité de s'échanger des informations et des liens. Lorsqu'on se connecte sur Twitter en tant que membre inscrit, on a accès aux tweets postés par ses followings c'est-à-dire les personnes que l'on a choisi de suivre. Par exemple, si l'utilisateur Elsa suit l'utilisateur Pierre, on dit qu'Elsa est un follower de Pierre alors que Pierre est un following d'Elsa. Twitter est un réseau social dit asymétrique à la différence de Facebook. Ainsi, il est possible qu'une personne choisisse de suivre très peu de ses followers. Notons qu'une personne ne souhaitant pas rendre trop publics ses messages peut parfaitement choisir de les rendre privés, visibles uniquement après validation d'une demande d'ajout à la liste des followers. Plus de 50% des utilisateurs actualisent leur profil soit à partir de leur mobile soit à partir d'outils autres que twitter (« outils dérivés » ex : Firefox propose un outil pour publier des infos sur twitter) (selon Sysomos –voir ci-dessous) Il est possible d'échanger directement avec des « amis » et décider que ses messages seront lus par tout le monde (mode public) ou seulement par son réseau (mode privé). Lors de la création d'un compte Twitter seuls sont demandés : un nom, un nom d'utilisateur, un mot de passe, une adresse mail ; Twitter conseille d'indiquer son vrai nom, son lieu de résidence si l'on veut être retrouvé par des amis mais il n'y a aucune obligation. Il est possible de modifier son profil ou de le créer avec ces paramètres : A TRADUIRE EN FRANCAIS….. En cochant la case "Protect my tweets": Only let people whom I approve follow my tweets. Si cette case est cochée : you WILL NOT be on the public timeline Tweets posted previously may still be publicly visible in some places.
L'utilisation	France / monde
Législation	La loi américaine s'applique. Par conséquent, aucune protection au sens de la législation en vigueur en France et en Europe ne parait reconnue par Twitter alors qu'aux fin de son service/traitement de données la société utilise des moyens (ici PC ou mobile) situé sur le territoire français (article 4 de la directive européenne de 1995 repris dans la loi informatique et liberté modifiée en 2004. Article 5§2 de Terms of service Protection du copyright
Statistiques concernant la population	France, juin 2009 : 10 000 à 12 000 inscrits selon Sysomos (société canadienne d'analyse des réseaux sociaux).

	Ce chiffre bien qu'encore très faible devrait augmenter de 190 % pour Paris. Selon Sysomos, parmi les utilisateurs de Twitter : • 31 % ont de 15 à 19 ans • 35 % ont de 20 à 24 ans • 15 % ont de 25 à 29 ans Notons que la simplicité d'utilisation, les différentes possibilités de connexions à savoir, internet et téléphone ainsi que la facilité d'enrichissement de l'outil font que le nombre d'utilisateurs croit très vite. Si le site était en français il est possible de supposer que le nombre d'inscrits français augmenterait considérablement. http://www.sysomos.com/docs/Inside-Twitter-BySysomos.pdf
Durée de conservation	La durée de conservation est inconnue.
Qui détient les données **Qui y a accès**	Les conditions générales d'utilisation de Twitter précisent en la matière : • « Nous engageons des prestataires de confiance pour des services d'hébergement de maintenance de relation clientèle, le stockage et la gestion de base de données et des campagnes de marketing direct. Nous partagerons vos données personnelles avec ces tiers, mais seulement à la mesure où elles sont nécessaires pour exécuter ces fonctions et seulement conformément dans le cadre d'obligations contractuelles qui les obligent à maintenir la confidentialité de vos données. » • « Twitter coopère avec le gouvernement et ses représentants ou des autorités privées chargés de faire respecter la loi. Nous pouvons communiquer n'importe quelles informations sur vous aux autorités publiques ou privées dans la mesure où nous seuls estimons, à notre seule discrétion, nécessaire ou approprié de répondre aux demandes légales, de protéger la propriété et les droits de Twitter ou d'un partenaire ou d'une personne privée, d'empêcher ou arrêter une activité illégale, contraire à la morale, ou légalement passible de poursuites judiciaires. » • « Nous nous réservons le droit de modifier ces conditions d'utilisation à tout moment. Si ces modifications constituent une modification matérielle des conditions d'utilisation, nous vous informerons par mail selon les préférences que vous avez indiquées dans votre compte. Ce qui constitue une "modification matérielle" sera déterminé à notre seule discrétion, avec bonne foi et en usant de bon sens et d'un jugement raisonnable. »
Droit de regard et rectification	Il est possible de modifier son profil à tout moment ainsi que de le supprimer. Twitter précise que les données indexées par des moteurs de recherche ne sont plus de son ressort. Si vous êtes répertorié comme utilisateur de Twitter vous pouvez avoir accès, mettre à jour ou corriger les informations données en envoyant un e-mail à l'adresse suivante privacy@twitterdot.com Un avertissement est donné quant à la suppression de données ou du profil : En effet, cette action est définitive. Dès lors, avant de procéder à la suppression, il faut que vous sachiez : • cette action est définitive et la remise en service du compte n'est pas possible • il n'est pas nécessaire que vous supprimiez votre compte pour changer votre nom d'utilisateur • votre compte peut être encore visible sur Twitter.com quelques jours après sa suppression • si vous souhaitez créer un nouveau compte et utiliser le même nom d'utilisateur, le même numéro de téléphone ou l'adresse mail associés à l'ancien compte, vous devez avant de le supprimer les modifier. Dans le cas contraire, ces informations ne seront pas valides et partant, inutilisables.

	• Nous n'avons aucun contrôle sur les informations répertoriées grâce à une recherche sur google
Dangers	Twitter collecte des données personnelles sur ses utilisateurs et les partage avec des tierces personnes. Twitter considère en effet ces informations comme un actif et se réserve ainsi le droit de les vendre si la société change de mains. Notons que les conditions générales d'utilisation précisent : « Nous nous réservons le droit de modifier ou mettre un terme aux services Twitter pour quelle que raison que ce soit, à tout moment et sans avertissement ». « Twitter peut vendre, transférer ou partager différemment tout ou partie de ses actifs y compris vos données personnelles à la suite d'une fusion, acquisition, réorganisation ou la vente d'actifs ou en cas de faillite. Vous aurez la possibilité de refuser un tel transfert si le traitement planifié par la nouvelle entité diffère matériellement de celui exposé dans les présentes politiques de confidentialité ». Twitter étant très bien référencé par les moteurs de recherches (en raison des mises en lignes incessantes des tweets) les données personnelles seront mises en avant par les moteurs de recherches (sauf si la case Protect my tweets a été cochée). Notons également qu'il est très voire trop aisé de pouvoir diffamer quelqu'un sur Twitter dans la mesure où il n'existe aucune surveillance instantanée.
Campagnes	Alertes ponctuelles lorsque des « incidents » surviennent, elles sont menées par des « veilleurs du Net » et non par les utilisateurs.
Recommandations	• Maintien du caractère personnel des données partagées. • Rendre les profils des utilisateurs inaccessibles par défaut aux moteurs de recherche. • Mener des campagnes auprès des pouvoirs publics (nationaux et européens) et des autorités de protections des données personnelles pour que TWITTER soit soumis au droit européen.

TÉLÉPHONIE

THEME	COMMUNICATIONS INTERPERSONNELLES Téléphonie Mobile
La technologie utilisée	**GSM-GPRS-3G-UMTS** Echange de messages, selon différents modes (voix, texte, images) entre personnes physiques (particuliers) à partir de téléphones mobiles/fixes et/ou d'ordinateurs. Cet échange est possible depuis n'importe où, dès lors que l'abonné a accès au réseau téléphonique de son opérateur ou d'un opérateur associé et notamment à l'étranger. Cela comprend : • Communication téléphonique (voix) • Visio communication • SMS (Short Message Service) : Message texte court (160 caractères) • MMS (Multimédia message service) : SMS auxquels on peut ajouter des photos, du son ou de la vidéo • GPS • Internet Mobile. • Messagerie électronique • Télévision L'intérêt d'un tel fichier : • Permettre aux opérateurs de conserver des données dans le contexte d'une relation commerciale avec les clients et de les transmettre uniquement à des tiers directement concernés par la facturation et le recouvrement. • Assurer la sécurité des réseaux et des installations. • Mettre les informations à la disposition des autorités judiciaires (réquisition judiciaire). • Facturation • Bonne marche du réseau • Recherche, constatation et poursuite des infractions pénales (Article R. 10-13 du Code des Postes et des Communications Electroniques) Dans tous les cas ci-dessus les informations retenues sont : • Informations permettant d'identifier l'utilisateur • Données relatives aux équipements terminaux de communication utilisés • Caractéristiques techniques, date, horaire et durée de chaque communication • Données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs • Données permettant d'identifier le ou les destinataires de la communication. • Données permettant d'identifier l'origine et la localisation de la communication
Pays et cadre d'utilisation	France / monde
Législation	Législation française : • Code des Postes et des Communications Electroniques (CPCE) : Livre II (partie législative, décrets en Conseil d'Etat, décrets simples).

	La tendance actuelle est à la suspicion généralisée à travers les lois Hadopi et Lopsi II (loi d'orientation et de programmation de la sécurité intérieure) ; une fois adoptées, elles renforceront les instruments légaux de surveillance et par conséquent on peut craindre un recul de la protection de la vie privée et des données personnelles en général et dans la téléphonie en particulier. • Loi informatique et libertés de 1978 modifiée en 2004. Conformité avec le droit européen : • Directive de 95 • Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») 2002/58/CE •
Statistiques concernant la population	Potentiellement toute la population. Selon une étude du Centre de Recherche pour l'Etude et l'Observation des Conditions de Vie (Credoc) (La diffusion des technologies de l'information et de la communication dans la société française (2008)), en juin 2008 78% de la population de plus de 18 ans était équipé de téléphonie mobile et 99% des 18/24 ans. En juin 2008, 69% des utilisateurs envoyaient des SMS avec leur téléphone portable, principalement les moins de 25 ans et les étudiants. Taux d'équipement personnel en téléphonie mobile (Credoc) : • novembre 2001 : 55% de population (et 84% des moins de 25 ans) • Juin 2008 : 78% de la population (et 99% des moins de 25 ans)
Fichiers générés et leur objet **Fichiers associés**	Source : Guide juridique pour les opérateurs locaux et les collectivités du 15 mars 2007 édité par l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes). Fichiers associés : • Fichier de gestion commerciale constitué par une entreprise privée (ici l'opérateur de téléphonie mobile), enregistrement des données d'inscription du client (voir Annexe 1 ART R10-14 I et II du CPCE - Code des Postes et des Communications Electroniques). • Fichier permettant d'assurer la sécurité du réseau et des installations (voir Annexe 1 ART R10-14 IV du CPCE) • Fichier des données de communications électroniques à conserver obligatoirement par les opérateurs de téléphonie mobile
Durée de conservation	1 an
Qui détient ces données ? **Qui y a accès ?**	La conservation des données peut être effectuée par l'opérateur ou confiée à des prestataires externes. • Les Salariés de l'entreprise qui conserve les données. • Les autorités judiciaires sur réquisition judiciaire. • S'agissant particulièrement de la prévention des actes de terrorisme, l'article L. 34-1-1 du CPCE prévoit le cas des réquisitions administratives qui permettent aux agents de la police et de la gendarmerie nationales habilités à cet effet d'obtenir communication de ces données auprès des opérateurs et des autres personnes mentionnées ci-dessus
Droit de regard et rectification	L'opérateur est tenu de veiller à préserver la sécurité des informations qu'il détient et qu'il traite. Dans ce cadre, il doit empêcher qu'elles puissent être déformées ou endommagées ou que des tiers non autorisés y accèdent. Les dispositions du CPCE rappellent qu'il est interdit de traiter les informations à caractère personnel en dehors des finalités déterminées, explicites et légitimes, qui permettent, notamment dans le domaine des communications électroniques, l'exécution d'un contrat auquel la personne qui fait l'objet du traitement est partie.

	Le droit d'accès et de rectification des clients aux informations nominatives les concernant qui sont traitées par l'opérateur est garanti. A ce sujet, les opérateurs veillent aussi à ce que leurs clients bénéficient des droits relatifs aux services d'annuaires et de renseignements téléphoniques. Il s'agit en particulier du droit de ne pas être mentionné sur les listes d'abonnés, de ne pas faire mention de l'adresse complète, d'interdire la prospection commerciale à partir de la liste ou d'empêcher la recherche inversée.
Dangers	• Spam • Sollicitations marketing (soumises normalement au consentement préalable de l'abonné) • Géo-localisation (soumise normalement au consentement préalable de l'utilisateur) • Rétention des informations de communication (une année) • Détournement des données pour d'autres finalités que celles prévues Conscience des dangers : Selon l'étude du Credoc concernant la **géo-localisation**, en 2008, 80% des 18-24 ans souhaitaient pouvoir interdire la transmission des données de leur localisation à des entreprises commerciales (les 12-17 ans n'étaient que 53%). 20 % des 18-24 ans en revanche ne souhaite pas avoir cette possibilité et 43% chez les 12-17 ans.
Campagnes	Existantes : inconnues A mener : • Campagne sur la géo-localisation (et publicité liée, notamment lors des voyages à l'étranger) • Campagne sur les données qui sont stockées par les opérateurs ou leurs mandants. Que deviennent-elles ? • Campagne sur le droit d'accès et de rectification Bonnes pratiques : • Eteindre son téléphone lorsque l'on ne s'en sert pas. • Lire attentivement les conditions générales. • Ne pas transmettre de donnée personnelle par SMS (Nom adresse, numéro de téléphone, numéro de carte bancaire, etc.). • Ne pas répondre à des SMS dont on n'est pas sûr de la provenance. • Ne pas suivre un lien transmis par SMS si on n'est pas certain de sa provenance. Concernant les SMS : l'ARCEP a mis en place un n° spécial pour lutter contre les SMS indésirables : **http://www.telecom-infoconso.fr/je-m-informe-sur/mobile/sms-indesirables.html** **Vous recevez un SMS indésirable : que faire ?** (Mise à jour le 16 décembre 2008) Depuis le 15 novembre 2008, les opérateurs ont lancé un dispositif de lutte contre les SMS indésirables : le "33 700". Ainsi, si vous recevez un SMS indésirable, vous incitant à composer de manière abusive un numéro surtaxé sans aucun service en contrepartie, transférez-le au 33 700. Pour plus de renseignements : www.fftelecom.org/files/CPtelecom.pdf
Recommandations	Obliger les opérateurs à rendre leurs Conditions Générales d'Utilisation accessibles, lisibles et complètes (ex : le numéro de lutte contre les spams mis en place par l'ARCEP n'est pas annoncé dans les CGU)

Réseaux Sociaux

F A C E B O O K

THEME	RESEAUX SOCIAUX
La technologie utilisée	FACEBOOK : Il s'agit d'un site web de réseautage social, crée en 2004 par Mark Zuckerberg et destiné à rassembler des personnes proches ou inconnues.
L'utilisation : pays et cadre d'utilisation	France / Monde La version française de Facebook a été mise en ligne en Mars 2008. L'inscription était initialement réservée aux étudiants de l'université de Harvard. Le site s'est progressivement ouvert à d'autres universités. Depuis 2005, Facebook s'est ouvert aux lycées. Depuis 2006, le site est accessible à tous.
Législation applicable et conformité avec le droit européen	Les conditions d'utilisation du site précisent que c'est la loi de l'Etat de Delaware qui s'applique. L'utilisateur accepte ces conditions dès l'instant où il s'inscrit sur le site. Concernant le droit européen : Le *Department of Commerce* américain, en particulier la *National Information Agency*, ont rapidement affirmé que la volonté américaine était, en ce qui concerne du moins le secteur privé, d'assurer une protection adéquate dans le cadre non d'une législation mais de codes de conduite et autres instruments d'autorégulation. Un premier texte qualifié d'« *Elements of Effective selfregulation for privacy Protection* » a été publié à ce propos en 1998. Suite aux négociations ininterrompues depuis 1998 entre la Commission européenne et les Etats-Unis, la position américaine a largement évolué. Le *Department of Commerce* du gouvernement américain a publié diverses versions des *Safe Harbor Principles* ou, selon la traduction française, des « *principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée* », qui visent à assurer la protection des données à caractère personnel transférées d'un Etat membre européen vers les Etats-Unis. La dernière version a été publiée le 17 mars. Par ailleurs, ces principes sont complétés par la réponse à des « QFP » ou, selon la terminologie américaine utilisée, à des « FAQ » (Questions Fréquemment Posées = *Frequently Asked Questions*), publiées par le Ministère du Commerce des Etats-Unis et fournissant des orientations pour la mise en œuvre de ces principes. Cependant, c'est toujours la loi Delaware qui s'applique et elle n'est pas aussi protectrice que la loi française en la matière.
Statistiques	Le site compte aujourd'hui 250 millions d'utilisateurs • 11,124,780 Français sont abonnés (la France est le 5e pays en nombre d'abonnés) • 3.665.000 pour les 18-24 ans soit 32,7% des abonnés. • 207.000 ont moins de 13 ans • 1.850.000 pour les 14-17 • 3.180.000 pour les 25-34 ans 600 000 à 700 000 comptes sont crées par jour dans le monde. 52% des Français qui possèdent un compte Facebook se connectent au moins une fois par semaine (25% le font quotidiennement) et la distribution au niveau des sexes et relativement équilibrée (52,2 % de femmes et 47,8% d'hommes. La popularité de Facebook a d'ailleurs bien augmenté puisque 68% des Français ont entendu parler de Facebook, ce qui représente une augmentation de 30% pour 2008 par rapport à 2007

Cadre d'utilisation	Il s'agit d'un moyen de communication.
Contenu	L'utilisateur entre en contact gratuitement avec d'autres utilisateurs
Intérêt d'avoir un compte Facebook	L'intérêt : • élargir son cercle d'amis • rester en contact avec ses proches, sa famille, ses amis • partager des vidéos, de la musique, des photos • possibilité de « chatter » grâce à une messagerie instantanée et privée L'utilisateur a la possibilité d'entrer des données personnelles et d'interagir avec d'autres utilisateurs. Les informations susceptibles d'être mises à disposition sur le réseau concernent l'état civil, les études et les centres d'intérêt. Ces informations permettent à l'utilisateur de retrouver ou de rencontrer d'autres utilisateurs partageant les mêmes centres d'intérêt. Ces derniers peuvent former des groupes et y inviter d'autres personnes. Le contenu du fichier est variable en fonction des utilisateurs. Chaque utilisateur choisit ce qu'il va partager avec les autres utilisateurs. Les informations dites « obligatoires » sont les suivantes : le nom, qui peut être un pseudonyme, le sexe, la date de naissance, qui peut être elle aussi inexacte ainsi que l'adresse mail. D'autres informations peuvent être indiquées : la religion, les opinions politiques, la formation professionnelle, les centres d'intérêt, l'employeur. Chaque utilisateur possède une page d'accueil où sont affichées les actualités concernant ses « amis », ainsi qu'une page propre « mur » où sont recensées ses actualités et où ses amis peuvent laisser des messages. Facebook propose à ses utilisateurs des fonctionnalités optionnelles appelées « applications ». Le choix des différentes applications à afficher est laissé à l'utilisateur, qui peut en ajouter après avoir consulté le catalogue. L'utilisateur pourra trouver sur sa page : • Une liste de ses amis • Une liste des amis qu'il a en commun avec d'autres amis • Une liste des réseaux auxquels l'utilisateur et ses amis appartiennent • Une liste des groupes auxquels l'utilisateur appartient • Une boîte pour accéder aux photos associées au compte de l'utilisateur • Un « mini-feed » résumant les derniers événements concernant l'utilisateur ou ses amis Les conditions générales (« terms of use ») de Facebook prévoient que l'utilisateur concède une licence à Facebook sur tout le contenu apporté par lui (« user content » : profil incluant nom et photo, messages, texte, information, photos, films…) Facebook peut également collecter des données à partir d'autres sources
Durée de conservation	- La Cnil s'est interrogée sur la durée de conservation des données récoltées par Facebook et ce dernier précise que cette conservation se fera durant une période « raisonnable » (« for a

	reasonable period ».) - Facebook conserve toutes les données personnelles partagées sur le site (inscrit dans les Conditions d'utilisation). Ainsi, un membre peut ***"décider de retirer ses contenus utilisateurs, entraînant l'expiration automatique de la licence qui a été accordée"***. Mais, Facebook précise que bien que n'étant pas propriétaire des contenus, il ***"reconnaît que la compagnie peut conserver des copies archivées des contenus générés"***. Facebook se justifie par le fait que cela facilitera l'éventuelle réinscription des membres qui ont abandonné le site, en leur évitant un réenregistrement de leurs données lors de leur réinscription. Pour supprimer son compte définitivement, il faut passer par un formulaire.
Détention des données **Droit de regard et rectification**	Chaque utilisateur peut, comme cela a été précisé précédemment, choisir ce qu'il désire partager. L'utilisateur de Facebook peut paramétrer la diffusion de son profil, des données permettant de le contacter et des applications dans l'onglet « Privacy settings ». C'est plus facile depuis que le site a été traduit en français. Il a également la possibilité de bloquer des personnes ou des groupes de personnes Il peut aussi bloquer partiellement ou totalement l'accès à son profil afin de ne pas apparaître dans les résultats des moteurs de recherche ou même dans les recherches sur Facebook (ainsi la saisie de ce nom sur Facebook n'aboutira à aucun résultat). Il n'y a pas de droit à l'oubli car les informations supprimées sont conservées par Facebook. Le droit de rectification n'est que superficiel car Facebook conserve toutes les informations postées sur le site et par ailleurs il est assez aisé de récupérer des informations même supprimées. En revanche, afin de pouvoir supprimer définitivement son compte facebook il est nécessaire de remplir un formulaire qui n'est d'ailleurs pas facile à trouver sur le site. Le plus souvent les utilisateurs ne font que suspendre leur compte.
Dangers	Facebook fait l'objet d'une controverse concernant le respect de la vie privée des utilisateurs. En effet, les informations sur la vie privée publiées sur Facebook peuvent être lues et utilisées par des personnes à qui elles n'étaient pas initialement destinées. Ainsi, certaines entreprises utiliseraient Facebook pour collecter des informations sur leurs employés tandis que les recruteurs s'en serviraient pour la sélection des candidats. Par ailleurs, certains parents utilisent Facebook pour surveiller la vie privée de leurs enfants. En outre, il est possible que le logiciel utilise les informations personnelles mise en ligne par l'utilisateur afin d'introduire des publicités adaptées à leur profil et vende les informations ainsi livrées à des entreprises privées comme c'est indiqué dans la charte concernant la vie privée. Cette charte précise que Facebook peut aller récolter des informations sur les membres à partir des sources extérieures tels que les journaux, les blogs ou d'autres sources Internet. De la même façon, les informations sur les utilisateurs sont collectées par Facebook afin d'améliorer ses bases de données et de permettre à ses clients de mieux cibler les publicités en connaissant les comportements et habitudes consuméristes de chaque utilisateur. Partant, les sites tiers peuvent, utiliser les informations récoltées par Facebook pour envoyer des publicités ciblées en fonction des différents profils. Polémique concernant *Beacon* : C'est le dernier logiciel publicitaire de Facebook en date qui permet à des sites Internet intégrant un script de facebook d'envoyer des informations sur les actions d'un membre sur leur site, aux amis de ce membre, dans leur « newsfeed » ou de mettre ces informations dans son journal sur sa page personnelle. Cette forme de marketing est considérée comme très efficace car elle passe par les réseaux sociaux et non par l'interpellation directe des personnes par la publicité. Face aux réactions suscitées par ce nouveau système publicitaire et à la menace qu'il représente, le créateur de Facebook a présenté ses excuses aux utilisateurs et a indiqué qu'au lieu du système *opt-out* au cas par cas (à chaque nouvelle intrusion, l'utilisateur de

	Facebook devait signifier à chaque entreprise qui fonctionnait avec *Beacon* qu'il ne voulait plus faire partie du système), ce serait à présent un système *opt-in* qui s'appliquerait où chaque utilisateur déciderait s'il intègre le système ou non. Notons également que les données personnelles peuvent être utilisées dans le cadre d'enquêtes judiciaires. Ainsi, pour connaître le profil privé d'un utilisateur ou son adresse IP, qui permet de le localiser, les enquêteurs doivent agir sur réquisition judiciaire à l'hébergeur du site **(**les comptes de 100 000 utilisateurs Facebook et MySpace ont déjà été supprimés à cause de soupçon de délinquance sexuelle)(4). Il existe plusieurs raisons pour supprimer un compte Facebook. Tout d'abord, Facebook peut vouloir éviter les SPAM (ainsi si on se rend compte que le même message est envoyé plusieurs fois à des individus différents, le compte pourra être supprimé) ou parce qu'on exerce une activité trop importante sur facebook (messages, photos etc). Facebook peut également supprimer le compte d'un utilisateur s'il a des doutes sur l'identité réelle de celui ci ou s'il a des doutes sur son école ou organisme d'affiliation ou s'il a écrit du contenu provocant. Cette suppression se fait de façon unilatérale sans explications.
Communications	Campagnes : Il n'y a pas de campagne de sensibilisation visant spécifiquement Facebook en France mais qui traitent de manière plus globale du réseau Internet en général et des réseaux sociaux en général. Ainsi, il existe une campagne menée par « reporters sans frontières » intitulée les ennemis d'Internet. Ce genre de campagne n'est pas connu du grand public et n'a donc pas un impact significatif. Les jeunes sont en général au courant des problèmes liés à Facebook. Il existe une tendance générale à paramétrer son profil afin d'en limiter l'accès aux inconnus. En outre, il existe une réaction assez généralisée pour dénoncer les dangers du fichage effectué par Facebook. Ainsi, un mouvement s'est créé sur Facebook qui s'intitule « Pas besoin d'EDVIGE, il y a déjà Facebook ». Cependant, de nombreuses ONG de défense des droits de l'homme et de la vie privée des personnes, comme *l'Electronic Frontier Foundation* ou *Privacy International*, s'inquiètent de cette nouvelle manière de récolter des informations sur les utilisateurs de tels sites et de les utiliser. Elle est considérée d'autant plus pernicieuse qu'elle se développe et se met en œuvre avec l'assentiment et la collaboration des utilisateurs de Facebook qui n'ont pas nécessairement conscience des dangers générés par de tels procédés. Il semblerait également que les employés de Facebook aient accès aux pages de tous les utilisateurs. Notons que fin novembre 2007, un réseau lancé par *MoveOn* a fait pression afin de défendre la vie privée des utilisateurs du site et a lancé une pétition en ligne demandant la suppression du système *Beacon..* Ainsi, de nombreux groupes se sont crées sur Facebook, dénonçant cette violation de la vie privée des utilisateurs du site. L'ascension de Facebook est inévitable car malgré les dangers qui existent pour certaines libertés fondamentales, ce réseau social reste très avantageux et pratique pour la plupart de ses utilisateurs.
Recommandations	Mener des campagnes auprès des pouvoirs publics (nationaux et européens) et des autorités de protections des données personnelles pour que Facebook soit soumis au droit européen. Par ailleurs demander la possibilité pour les utilisateurs de Facebook : • d'une clôture définitive du compte incluant par là-même une suppression de toutes les données personnelles partagées. • de rendre les profils des utilisateurs inaccessibles par défaut aux moteurs de recherche.

COPAINS D'AVANT

THEME	RESEAUX SOCIAUX : COPAINS D'AVANT
La technologie utilisée	Il s'agit d'un site Web français de réseautage social appartenant au Benchmark group. Il a été créé en 2001et permet aux utilisateurs de retrouver d'anciens camarades qui ont partagé leur scolarité ainsi que leurs activités professionnelles, associatives ou de loisir. L'inscription sur le site de copains d'avant permet aux inscrits de consulter les profils des membres. Elle est subordonnée au remplissage d'un formulaire mentionnant l'identité de la personne ainsi que les différents établissements fréquentés. En vous inscrivant sur l'Internaute Copains d'avant, vous renseignez des informations vous concernant dans divers formulaires du site. Ces informations, comme votre adresse mail ou votre parcours scolaire, sont nécessaires pour utiliser correctement le site, mais elles sont avant tout des données qui sont personnelles et donc précieuses. Le site dispose d'une messagerie électronique interne et propose un partage de photos. La messagerie du site est gratuite et seules quelques options marginales sont payantes telles que l'extension de l'espace de stockage à 1 Go pour les photos et 2 Go pour les vidéos ainsi que la possibilité de publier des avis de recherche illimités et d'adresser des messages à plusieurs membres à la fois. En 2008, le site inaugure de nouvelles fonctionnalités gratuites inspirées de celles proposées par Facebook et MySpace. En effet, il est désormais possible à chaque membre d'afficher ses goûts culturels et de voir quels autres membres les partagent.
L'utilisation	France. Le but est de rester en contact ou de retrouver d'anciens camarades de classe.
Législation	• Les sites Internet sont soumis à la loi sur la presse, loi sur la communication audiovisuelle et à la LCEN. • La loi Informatique et libertés s'applique mais ils sont dispensés de déclaration à la Cnil lorsqu'ils contiennent des données à caractère personnel (cependant il ne faut pas oublier que pour la publication de données à caractère personnel, un autorisation est souvent demandée pour les moins de 12 ans). • Enfin, la loi du 21 juin 2004 qui définit le régime d'identification en ligne s'applique, ainsi l'anonymat ou le pseudo sont autorisés tant que l'hébergeur détient l'identité de la personne et peut la transmettre à l'autorité judiciaire. La jurisprudence évolue vers une responsabilité des hébergeurs car ce sont eux qui offrent des plateformes de plus en plus adaptées aux contenus. Copains d'avant est soumis à la législation française et par conséquent à la législation européenne. Application des directives européennes.
Statistiques concernant la population	Dix millions de personnes étaient inscrites en 2008, ce qui en faisait le premier site de réseau social en France. En outre, selon une étude IFOP parue dans les Echos en 2009, Copains d'avant devance encore Facebook lorsque l'on recense le nombre d'inscrits au sein de la population internaute française.
Durée de conservation	Pas d'information
Qui détient ? **Qui y a accès ?**	Possibilité de restreindre l'accès à nos données personnelles. les profils sont consultables par les autres inscrits (sauf restrictions) et on peut effectuer des recherches par mots-clés (nom de lycée, de ville etc.) Les fichiers sont partagés avec des sites tiers. En effet les données personnelles font l'objet

	d'une publicité ciblée.
Droit de regard et rectification	Les utilisateurs peuvent restreindre leurs profils ou supprimer certaines informations.
Dangers	Copains d'avant ayant un public un peu plus âgé que d'autres réseaux sociaux, les utilisateurs sont un peu plus conscients des problèmes liés à la mise en ligne d'informations personnelles. En outre, un utilisateur ne se servira pas de cette plateforme pour une durée aussi longue que sur d'autres réseaux sociaux ; ainsi, après avoir retrouvé des amis, la fréquentation décroit. Soucieux de protéger la vie privée des membres, Benchmark Group, éditeur de Copains d'avant, met à votre disposition de nombreux outils : • Votre adresse e-mail n'est jamais révélée sur le site • Si vous ne souhaitez pas rendre publique la totalité de votre fiche, vous pouvez contrôler qui est autorisé à y avoir accès et quelles informations seront publiques ou non. • Il vous est également possible de limiter l'accès à vos albums photo • Il vous est possible de filtrer certains messages • Vous pouvez en outre signaler un abus si vous constatez des comportements répréhensibles sur le site. • Vous pouvez choisir que les moteurs de recherche ne puissent pas référencer votre page • Vous pouvez souhaiter ne pas apparaître sur JDN réseau • Il vous est possible de supprimer votre compte • Enfin, les fichiers Copains d'avant sont déclarés auprès de la CNIL
Communications	Pas de campagne
Recommandations	

MYSPACE

THEME	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 faire un blog. Le site possède également un système de messagerie et permet de mettre 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. Depuis mi-juillet il existe une version française du site. 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…).
L'utilisation	France Monde
Législation	• Loi fédérale américaine. • Myspace a adhéré au système Safe Harbour qui repond 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 : **Conditions d'utilisation :** 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'est pas 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 États-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. 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 communautaire étant de plus en plus large. L'attrait des sites communautaire 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 se connectent 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 notre profil. Si le profil n'est pas bloqué tout le monde peut y accéder (sans restrictions d'ordre géographique par exemple) • email 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 à qui aura le plus de contacts semble exister donc, il n'existe pas vraiment de tri dans ses 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 ». Ces campagnes ne sont pas connues du grand public et n'ont par conséquent pas un impact significatif sur les populations concernées. Réaction pour dénoncer le fichage effectué par Myspace, notamment via des articles de presse ou des groupes de mécontentement 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.

F L I K R

THEME	RESEAUX SOCIAUX
Technologie utilisée	Il s'agit d'un site Web de partage de photos et de vidéo gratuit comprenant certaines fonctionnalités payantes. Flickr ne se contente pas d'être un site Web uniquement populaire auprès des utilisateurs pour partager leurs photos personnelles, il est aussi souvent utilisé par des photographes professionnels. Flickr est lancé en 2004 par une société canadienne de Vancouver fondée en 2002 par Stewart Butterfield et Caterina Fake. Flickr était initialement un ensemble d'outils prévus pour un jeu informatique multiutilisateurs sur internet, *Game Neverending.* Le jeu fut finalement abandonné mais pas le projet Flick. Les premières versions de Flickr étaient fondées sur une *Chat room* afin de partager des photos. Ultérieurement, Flickr s'est concentré plus précisément sur le téléchargement et le classement des photos. Flickr appartient à Yahoo depuis 2005. Longtemps uniquement disponible en anglais, Flickr propose depuis 2007 7 langues supplémentaires. L'objet principal est le partage de photos et de vidéos. C'est également devenu une plateforme de blogging. L'ouverture d'un compte requiert l'adhésion à Yahoo! Mail (ce qui implique de fournir toutes sortes d'informations). Les profils des adhérents font également l'objet d'une publicité ciblée. Les informations fournies lors de l'inscription et lors du téléchargement des photos (tags) sont utilisées par Yahoo! pour cibler les annonces publicitaires. Il existe un système de censure des photos qui pourraient prêter à controverses. Notons que le site permet à la fois un stockage public et privé. Ainsi, un utilisateur chargeant une image sur le site peut déterminer qui aura accès à son image en réglant les contrôles d'accès. Ces réglages peuvent être catégorisés privés, pour les amis, la famille ou bien public. Il est aussi possible d'effectuer des réglages privés pour tout un groupe. Cependant, la plupart des utilisateurs rendent leurs photos publiques, pouvant ainsi être vues par tout le monde et formant par là même une très grande base de données de photos rangées par catégorie. Par défaut, les autres utilisateurs peuvent laisser des commentaires sur toute image qu'ils ont le droit de voir et parfois peuvent ajouter des mots-clés pour cette image. Concernant l'utilisation même de Flickr, notons que les photos sont balisées (tags) ce qui permet une recherche plus facile par mots-clés De même, les photos peuvent être organisées dans des groupes ce qui permet une recherche plus facile. En outre, il existe un système de « guest pass » qui permet de partager des images avec des personnes qui n'ont pas de compte flickr.
L'utilisation	États-Unis/Monde
Législation	Les données sont transférées auprès de Yahoo! Inc. sur ses serveurs aux États–Unis, ou

	dans d'autres pays, en vue de leur traitement ou de leur stockage, à l'occasion de l'utilisation de services offerts sur des sites Yahoo! autres que le site Yahoo! France, ce à quoi les utilisateurs consentent expressément en validant le formulaire de création de compte Yahoo!. Le transfert aux États-Unis des données personnelles, a fait l'objet d'un accord entre Yahoo! Inc. et Yahoo! France pour garantir la protection des données des utilisateurs. La base de données constituée par les données de création de comptes Yahoo! a fait l'objet d'une délcaration auprès de la CNIL. Ces informations étant protégées par le secret professionnel, Yahoo! ne pourra les communiquer que sur réquisition d'une autorité judiciaire ou administrative habilitée française, ou rattachée à l'État dans lequel elles sont traitées et/ou stockées.
Statistiques concernant la population	• 20% des utilisateurs possèdent 82% des photos du site et les 3,7% d'utilisateurs ayant un compte « pro » (payant) ont mis en ligne 59,5% des images. • 62% des gens n'ont aucune photo, • 65% n'ont aucun contact, • 87% n'ont jamais posté de commentaire, • 84% n'en ont jamais reçu, • 93% n'ont choisi aucun « favori ». • 92% ne participent à aucun groupe. • Au final, seuls 3% des utilisateurs utilisent toutes les fonctionnalités de Flickr. Même chez les « pro », certains usages sont minoritaires. C'est le cas des favoris (56% n'ont jamais choisi de favori) et des groupes (49% des pros y participent). Aucun chiffre communiqué concernant la France spécifiquement.
Durée de conservation	Aucune information
Qui détient ? Qui y a accès ?	Yahoo! déclare la collecte et le traitement des données personnelles auprès de la CNIL.
Droit de regard et rectification	Conformément à la Loi du 6 janvier 1978 modifiée, dite Loi Informatique et Liberté, les utilisateurs disposent en ligne d'un droit de consultation, de modification et de retrait des toutes données personnelles collectées par Yahoo!
Finalité du fichier	Partage de photos et de vidéos
Dangers	Les dangers sont principalement liés au droit à l'image et au risque de retrouver des photos en ligne sans l'accord de la personne photographiée. Nous avons dit que les utilisateurs avaient le choix entre rendre leurs photos publiques ou les maintenir privées. Le plus souvent les utilisateurs rendent leurs photos publiques ce qui constitue une énorme base de donnée et un risque d'autant plus grand pour la vie privée. Il existe également un risque d'espionnage, d'utilisations calomnieuses de photos. Notons que la plupart des utilisateurs n'ont pas conscience des problèmes car le partage des photos est large ; les utilisateurs ont dès lors l'impression de moins se dévoiler que sur d'autres réseaux sociaux car l'accent n'est pas mis sur des informations personnelles telles que le lieu d'étude ou de résidence.
Campagnes	Il n'existe pas de campagne de sensibilisation. Il faudrait sensibiliser les jeunes sur les conséquences futures de mettre des photos sur Internet sans la permission des personnes photographiées. De plus en plus d'employeurs recherchent sur Google les noms des différents postulants à un travail et peuvent par conséquent retrouver des informations contenues sur des réseaux sociaux.
Les bonnes pratiques	Il est possible de paramétrer son profil afin de ne pas exposer son profil à des inconnus.

	Notons qu'il existe une licence pour protéger ses photos, le Creative Commons qui est un service payant. Précisons que l'accès à la justice concernant des litiges relatifs au droit à l'image est souvent difficile et coûteux.
Recommandations	Mener des campagnes de sensibilisation.

SKYROCK BLOG

THEME	RESEAUX SOCIAUX : SKYROCK BLOG
La technologie utilisée	Il s'agit d'un site de réseau social mettant gratuitement à disposition de ses membres un espace Web personnalisé. Le site est lancé le 17 décembre 2002 par la radio française Skyrock. Il est également possible d'y faire un blog, y ajouter un profil et échanger des messages avec les autres membres. Le site permet de créer des blogs dédiés aux compositions musicales des membres et consacre un espace spécifique à ces créations. Chaque blog peut être personnalisé et il est possible d'intégrer des vidéos mais uniquement si elles proviennent de Youtube, Dailymotion, Veoh, Metacafe, Google Video ou de sa webcam. Depuis 2006 (après l'arrivée de Myspace et Facebook), Skyrock Blog s'est doté d'un système de liste d'amis et de liste de contacts qui s'affiche sur le blog et qui permet d'établir des liens réciproques entre les membres. Notons également le lancement de Skyblog Music qui sur le modèle de Myspace permet aux bloggeurs de diffuser de la musique. Il existe une plateforme de conversation, SkyMessager ainsi qu'une plateforme pour gérer ses emails, Skymail. Ces améliorations apportées au système Skyblog permettent de concurrencer les grands réseaux sociaux américains et de garder les utilisateurs sur ce site.
Cadre d'utilisation	France / Europe
Législation	Skyrock blog est soumis à la législation française et par conséquent à la législation européenne. Application des directives européennes. Les blogs constituent un service de communication en ligne et sont donc soumis à la même législation que les sites Internet à savoir la loi sur la presse, la loi sur la communication audiovisuelle, et la loi pour la confiance de l'économie numérique. La loi Informatique et libertés s'applique mais il n'est pas nécessaire d'effectuer une déclaration à la Cnil lorsque les blogs contiennent des données à caractère personnel. Cependant, il ne faut pas oublier que, pour la publication de données à caractère personnel, une autorisation est souvent demandée pour les moins de 12 ans. Enfin, la loi du 21 juin 2004 qui définit le régime d'identification en ligne s'applique, ainsi l'anonymat ou le pseudo sont autorisés tant que l'hébergeur détient l'identité de la personne et peut la transmettre à l'autorité judiciaire. Précisons qu'il est toujours difficile de savoir s'il faut condamner l'éditeur ou l'hébergeur qui peuvent être de nationalités différentes ce qui peut entrainer des difficultés quant à la législation applicable. La jurisprudence évolue vers une responsabilité des hébergeurs car ce sont eux qui offrent des plateformes de plus en plus adaptées aux contenus.
Statistiques concernant la population	Le site se situe à la 17ème place mondiale devant Wikipedia et Amazon et représente 27% des blogs français. La population ciblée est celle des 12-24 ans. Très populaire auprès des collégiens et des lycéens car il est simple d'utilisation. Notons que 15 millions de blogs étaient recensés en avril 2008. Au 7 mars 2009 la plateforme Skyblog comptait 23 000 000 blogs et 637 600 000

	articles.
Durée de conservation	Aucune information.
Qui détient les données ? **Qui y a accès ?**	Les fichiers sont partagés avec des sites tiers. En effet les données personnelles font l'objet d'une publicité ciblée. Notons que les publicités sont contextualisées par rapport au contenu de la page Skyblog. Ainsi mieux ciblée, la publicité est plus efficace.
Droit de regard et rectification	En conformité avec les dispositions de la loi N° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés, le site Skyblog fait l'objet d'une déclaration à la CNIL, sous le n°895721 en date du 23 janvier 2004. Les utilisateurs ont un droit d'accès, de modification, de rectification et de suppression des données qui les concernent (art. 34 de la loi 'Informatique et Libertés' du 6 janvier 1978).
Dangers	• espionnage et délinquance sexuelle. • utilisation des informations contenues dans le blog pour des enquêtes judiciaires. • Un Skyrock Blog contient parfois des éléments protégés par le droit d'auteur sans l'accord des ayant-droits, Certains skybloggeurs vont même jusqu'à porter des propos graves sur certaines personnes : plusieurs collèges ont dû faire face à des problèmes concernant des élèves utilisant la plateforme pour porter atteinte au personnel, entraînant des exclusions et des alertes largement diffusées aux élèves et aux parents. • Notons que le tribunal administratif de Clermont-Ferrand a annulé l'exclusion d'un élève par le corps enseignant après que celui ci ait insulté un de ses professeurs sur son blog. L'école et les blogs sont tous deux des espaces privés, au sens où les activités qui s'y déroulent ne sont pas destinées à un public élargi, mais à ceux qui s'y reconnaissent. Ainsi le blogging, qui est un espace en cours d'institutionnalisation, doit pouvoir être autonome vis-à-vis de l'école.
Communication	Conscience des dangers : • Il semblerait que les skybloggeurs et en particulier les plus jeunes, ne soient pas conscients, d'une part, des dangers de la diffamation (quel que soit le support), et d'autre part, de la critique extérieure d'une certaine communauté de passionnés de l'informatique et de bloggeurs (utilisant des plateformes considérées plus sérieuses et puissantes, comme le logiciel libre DotClear) face aux Skyrock Blogs. • Réaction des parents ou de la presse en général. Les utilisateurs ne sont pas aussi réactifs que pour d'autres réseaux comme Myspace ou Facebook.
Campagnes	Il n'y a pas de campagne spécialement destinée à Skyrock Blog.
Recommandations	Il faut sensibiliser les jeunes aux risques encourus par la publication d'images ou de textes sans autorisation ou diffamatoire. Par ailleurs les moyens de paramétrer son profil ne sont pas aussi performants que ceux d'autres réseaux sociaux. En outre, lorsqu'on appréhende un contenu illicite sur un blog il est souvent difficile de distinguer entre le droit civil et le droit pénal car les expressions utilisées ne sont pas toujours claires. L'utilisateur n'est pas toujours suffisamment au courant des conséquences de ses actes et des dangers liés à partage trop important de ses données personnelles.