



**Conseil Général de l'Industrie,
de l'Énergie et des Technologies**

Internet et le respect de la vie privée

Rapport présenté par

**Jean-Claude GORICHON, Contrôleur général économique et financier
Dominique VARENNE, Contrôleur général économique et financier
Maurice SPORTICHE, Administrateur civil HC – Chargé de mission**

Avec la participation de

**Lionel ARCIER, Contrôleur général économique et financier
Jean-Gervais BIART, Contrôleur général économique et financier
François CHOLLEY, Ingénieur général des Mines
Jean CUEUGNIET, Ingénieur général des Mines**

RAPPORT N° IV-1.9-2008 – Mars 2009

Rapporteurs :

Jean-Claude GORICHON,
Contrôleur général économique et financier
Dominique VARENNE,
Contrôleur général économique et financier
Maurice SPORTICHE,
Administrateur civil HC – Chargé de mission

Avec la participation de

Lionel ARCIER,
Contrôleur général économique et financier
Jean-Gervais BIART,
Contrôleur général économique et financier
François CHOLLEY,
Ingénieur général des Mines
Jean CUEUGNIET,
Ingénieur général des Mines

Internet et le respect de la vie privée

SYNTHESE

Le développement d'internet et des multiples services offerts en ligne a pour corollaire la multiplicité des données recueillies auprès des internautes, de façon volontaire pour les besoins des transactions effectuées, ou à leur insu, par des acteurs divers ayant pour objectif de tracer le profil des internautes. Face à cette situation qu'ils ne peuvent que difficilement contrôler, l'inquiétude grandit parmi les internautes sur les atteintes à leur vie privée que constituent la conservation de données personnelles et leur usage.

Le respect de la vie privée des internautes est un sujet qui comporte de multiples facettes et le présent rapport a choisi de privilégier les aspects relatifs à la consolidation des données et au secret des correspondances. Compte tenu de la complexité du sujet due à la multiplicité des acteurs et des situations ainsi qu'au caractère mondial d'Internet, le rapport a seulement esquissé des pistes de réflexion pour répondre aux abus les plus criants, sans prétendre pouvoir résoudre l'ensemble des problèmes ; celles-ci devraient être approfondies et portées au niveau européen.

Après un constat des différents acteurs ainsi que des différents types de données recueillies (anonymes ou nominatives, volontaires ou à l'insu de l'internautes), le rapport expose les risques pour la vie privée qui naissent des pratiques des acteurs.

La consolidation des données, qui permet à partir de données anonymes ou nominatives de dresser un profil complet des internautes, et l'utilisation des robots de messagerie qui relèvent des mots clés dans les messages transmis ont été mis en exergue, à côté de pratiques elles aussi problématiques comme les cookies, les scripts ou les logiciels espions.

Le rapport constate que les protections actuelles, qu'elles soient techniques ou juridiques sont insuffisantes, soit qu'elles soient peu connues (par exemple les anonymiseurs) ou difficiles à mettre en œuvre (caractère national de la loi, moyens de contrôle et de sanctions peu adaptés). Les pistes de proposition relèvent de deux principes :

- l'affirmation d'un véritable droit à l'anonymat et à la transparence sur l'usage des données recueillies,
- le respect du secret des correspondances.

L'affirmation d'un droit à l'anonymat a donné lieu aux propositions suivantes :

- introduction dans le droit positif pour les fournisseurs de service d'une obligation passible de sanction, de recueillir auprès des internautes des autorisations explicites et graduées pour l'utilisation de leurs données nominatives ;
- introduction de clauses contractuelles type obligatoires concernant l'effacement des données pour les fournisseurs de services français qui contractent avec les consolidateurs de données ;
- créer un statut juridique des données personnelles par secteur d'activité (données médicales, bancaire, état-civil, droit des marques ..) ;
- rappel aux personnels des FAI les obligations qui s'attachent au secret des correspondances et les sanctions prévues.

Le respect du secret des correspondances est réaffirmé face aux robots de messagerie et il est proposé d'interdire l'usage des robots et automates analysant ou collectant des données personnelles dans les messages électroniques pour les fournisseurs de service de communications électroniques.

Au-delà de ces deux principes majeurs, d'autres mesures ont été envisagées pour renforcer la protection de la vie privée des internautes :

- mieux organiser le contrôle effectif des pratiques illicites par une coordination des différents services chargés de ces tâches et par une adéquation des moyens affectés à ces tâches, (création d'un service spécialisé, renforcement des sanctions) ;
- clarifier et simplifier le régime des labels concernant internet en en confiant le pilotage à un seul acteur (CNIL par exemple), étudier la faisabilité de la création d'un label de bonne conduite en matière de respect de la vie privée ;
- renforcer l'information des utilisateurs d'Internet sur les avantages et les risques des outils numériques par la CNIL ou une autre entité ;
- faire organiser (par la DGCIS du MEIE par exemple) un concours pour créer le mur anti-feu des données personnelles propres à chaque internaute ;
- encourager l'Europe à renforcer les obligations qui devraient peser sur les acteurs en matière de recueil et d'exploitation de données personnelles.

SOMMAIRE

A - LE CONSTAT	2
I. UNE DIVERSITE D'ACTEURS INTERVIENT TOUT AU LONG DE LA CHAINE DE COMMUNICATION	2
II. DES DONNEES DIFFERENTES RECUEILLIES PAR CES ACTEURS	4
II.1. Les données nécessaires pour le simple acheminement de la communication.....	4
II.2. Typologies des données recueillies.....	4
III. DES DONNEES UTILISEES PAR LES ACTEURS AU-DELA DE LA STRICTE NECESSITE DE LA COMMUNICATION DE LA CONSULTATION OU DE LA TRANSACTION	6
IV. DES UTILISATIONS QUI POSENT PROBLEME AU REGARD DU RESPECT DE LA VIE PRIVEE	6
IV.1. La consolidation des données.....	6
IV.2. Les robots de messagerie.....	7
IV.3. Les moyens techniques divers	8
V. DES RISQUES FORTEMENT ACCRUS D'ATTEINTE A LA VIE PRIVEE DES UTILISATEURS	14
V.1. Des données a priori impersonnelles peuvent aisément être personnalisées.....	14
V.2. Des données nominatives insuffisamment protégées	14
VI. DES PROTECTIONS RELATIVEMENT INSUFFISANTES FACE A CES RISQUES	15
VI.1. Des protections techniques individuelles mal connues voire limitées.....	15
VI.2. Une protection juridique insuffisante dans son application effective voire dans son champ	18
B - PISTES DE PROPOSITIONS A APPROFONDIR	21
VII. L’AFFIRMATION D’UN VERITABLE DROIT A L’ANONYMAT ET DROIT DE SAVOIR	21
VII.1. Cas de la consultation d’un site	21
VII.2. Cas des consolidateurs de données.....	22
VII.3. Cas des gestionnaires d'identifiants personnels.....	22
VII.4. Cas des FAI	23
VIII. LE RESPECT DU SECRET DES CORRESPONDANCES : CAS DES ROBOTS DE MESSAGERIE	23
IX. AUTRES DISPOSITIONS COMPLEMENTAIRES POUVANT ETRE ENVISAGEES	24
IX.1. Organiser le contrôle- application de la législation et de la réglementation, conformité des chartes de déontologie	24
IX.2. Etudier la faisabilité d’un label de bonne conduite en matière de respect <i>de la vie privée pour les prestataires de services</i>	24
IX.3. Renforcer l’information des utilisateurs.....	25

Internet et le respect de la vie privée

Que ce soit pour les usages privés ou professionnels, la multitude de services offerts par internet entraîne une explosion des données qui transitent par ce canal désormais point de passage privilégié, voire incontournable.

Cela n'est cependant pas sans poser un certain nombre de problèmes concernant la confidentialité des informations transportées, leur fiabilité et le « traçage automatique » de l'internaute. Les risques relatifs à cet égard ne sont pas simplement des risques techniques, qui existent par ailleurs, mais sont liés au comportement potentiel des acteurs présents sur la chaîne de valeur des services Internet et au mode de financement par la publicité de certains services.

Parmi ces interrogations, un des aspects qui tend à susciter de plus en plus d'inquiétude porte sur la question du respect de la vie privée des internautes. Une étude du CREDOC menée en 2008 pour le compte de l'ARCEP et du CGTI met en évidence que 60% des internautes se sentaient préoccupés par la question de l'utilisation des données qu'ils fournissaient, spontanément ou non, auprès des divers acteurs présents sur la Toile. Les rapporteurs ont ainsi rencontré plusieurs associations de consommateurs qui commencent à s'inquiéter des dérives possibles.

L'accroissement de cette inquiétude est surtout lié au risque démultiplié par les nombreuses possibilités de recoupage des informations recueillies, mais aussi par une prise de conscience croissante des risques d'atteinte à la vie privée.

Face à cette inquiétude légitime qui touche au respect de la vie privée de chacun, le présent rapport a pour objet d'analyser les comportements des principaux acteurs de l'Internet, que ce soit dans l'utilisation des informations recueillies ou dans les dérives potentielles. Le champ d'investigation s'est focalisé sur deux aspects essentiels liés à cette problématique: la correspondance privée sur Internet et la consolidation des données. Les aspects liés aux réseaux sociaux qui sont également porteurs de difficultés relatives au respect de la vie privée, n'ont pas été examinés par les rapporteurs dans la mesure où ces sujets font déjà l'objet d'une attention soutenue de la part d'autres acteurs institutionnels comme la CNIL.

Les rapporteurs ont rencontré à cet effet un certain nombre d'acteurs importants d'internet pour mieux cerner les différentes méthodes utilisées pour le fonctionnement des sites marchands ou d'information (cf. liste en annexe 1). Enfin la CNIL a été contactée pour évoquer l'approche retenue et sa complémentarité avec celle de cette institution.

Compte tenu de l'ampleur et de la complexité du sujet les rapporteurs sont conscients de ne pouvoir apporter de réponses complètes et définitives aux problèmes rencontrés mais ont essayé de tracer des pistes de réflexion qui mériteraient d'être approfondies par l'ensemble des acteurs concernés.

A - LE CONSTAT

I. UNE DIVERSITE D'ACTEURS INTERVIENT TOUT AU LONG DE LA CHAINE DE COMMUNICATION

Les communications vers Internet font intervenir des acteurs divers dont le rôle et les obligations sont extrêmement diversifiés, ce qui n'empêche pas des entreprises de jouer plusieurs rôles à la fois. Schématiquement on peut définir ainsi les principaux acteurs :

Les acteurs techniques :

Les fournisseurs d'accès à Internet (FAI) : ils permettent l'accès à internet au moyen du raccordement de l'utilisateur à leur réseau, ils acheminent en général les communications

Exemple : FT-Orange, Neuf-Cegetel, Free, etc.

Les hébergeurs :

Ceux-ci peuvent proposer une prestation plus ou moins complète. On désigne sous ce nom à la fois les entreprises qui mettent à disposition des fournisseurs de service des locaux vides d'informatique mais « prêts à l'emploi », c'est-à-dire raccordés au réseau, climatisés, alimentés en énergie, etc. et des entreprises qui gèrent l'environnement technique et les serveurs informatiques pour le compte des fournisseurs de services.

Exemple: OVH, Amen, RedHouse, Téléhouse, Orange, etc.

Les fournisseurs de services de communications électroniques :

Concernant internet cette catégorie recouvre essentiellement les fournisseurs de services de messagerie électronique, qui peuvent par ailleurs avoir d'autres fonctions.

Exemple: Orange, Google mail, Yahoo Mail, etc.

Les fournisseurs de services au public en ligne, assimilés souvent à des éditeurs

Sous cette appellation on trouve les fournisseurs de services du secteur marchand, gratuits ou non : : vente par correspondance, vente aux enchères, sites financiers, presse, etc., ainsi que les fournisseurs de la sphère non marchande : administrations publiques et institutions diverses. Les moteurs de recherche font également partie de cette catégorie.

De la même façon les fournisseurs de « réseaux sociaux » appartiennent à cette catégorie de même que les différents fournisseurs de blogs, forums, ...

Exemple: www.service-public.fr, lemonde.fr, fnac.com, etc.

Les consolidateurs des données recueillies.

Ces acteurs ne sont pas directement accessibles par les internautes mais agissent pour le compte des fournisseurs de services qu'ils soient de communications électroniques ou de services au public en ligne.

Exemple: Doubleclick, Cybermonitor, Overture, SmartAdserver, Google-analytics, etc.

Les gestionnaires d'identifiants et de données personnelles.

Contrairement aux précédents, ces acteurs sont directement accessibles par les internautes auxquels ils proposent des services utiles, mais à ce jour très mal encadrés, de gestion de tout ou partie de leurs des données personnelles, plus ou moins sensibles (des données médicales aux avatars) afin de faciliter la mémorisation, mais aussi d'accélérer les connexions, voire de renseigner automatiquement les champs des questionnaires en ligne.

Exemple: Google, Passport de Microsoft, Open ID, le futur opérateur des données médicales français, etc.

Compte tenu de leur positionnement différent dans la chaîne de la communication, ces différents groupes d'acteurs ne font pas appel au même type de données qualifiant l'internaute qui visite les sites.

II. DES DONNEES DIFFERENTES RECUEILLIES PAR CES ACTEURS

II.1. Les données nécessaires pour le simple acheminement de la communication

Les acteurs techniques recueillent essentiellement des données techniques nécessaires à l'établissement et l'acheminement de la communication :

Les FAI fournissent une adresse IP à l'internaute lors de sa connexion et acheminent celle-ci jusqu'au site demandé ou jusqu'au fournisseur de messagerie concerné. D'autres données sont également transmises lors de la communication : codes divers, caractéristiques liées à l'accès au service (heure, date, fuseau horaire, durée, ...), caractéristiques liées à son équipement (type O/S, marque de navigateur,...).

Les hébergeurs techniques gérant les serveurs reçoivent a minima les adresses IP des internautes qui cherchent à atteindre leurs sites.

Les gestionnaires de messagerie sont dépositaires des contenus des messages arrivés et voient passer les messages émis.

Les fournisseurs de services au public en ligne sont susceptibles quant à eux de recueillir toutes les données que leur transmettent les internautes lors de la consultation de leur site. Toutefois s'il est nécessaire au fonctionnement même d'internet et des services offerts que des données soient déposées et acheminées sur le réseau ou sur les sites, il faut prendre en considération que des informations complémentaires peuvent être induites par la visite de ces sites et que des comportements portant préjudice au respect de la vie privée peuvent être observés. De la même façon l'injection d'informations non demandées peut également porter atteinte à la vie privée par un mécanisme décrit ci-après.

L'ensemble de ces données n'a pas la même importance pour l'utilisateur d'Internet ni le même rôle pour les différents acteurs de l'internet.

En effet, ces nombreuses données peuvent être anonymes ou non, être récupérées, transférées à des tiers, et être stockées pour des durées plus ou moins longues, en pleine connaissance ou à l'insu de l'utilisateur.

II.2. Typologies des données recueillies

II.2.1. Des données anonymes ou non

Une première typologie consiste à différencier les données selon leur caractère anonyme ou non.

- **Les données nominatives :**

Il s'agit soit de données comportant l'état civil réel de la personne, éventuellement de ses coordonnées. Il peut s'agir aussi des données techniques qui ne permettent pas

immédiatement d'identifier cette personne mais peuvent permettre de retrouver cette identité. C'est notamment le cas de l'adresse IP, qui fait partie des données nécessaires à l'acheminement de la communication mais permet d'identifier l'abonné utilisant la connexion ou de cerner les utilisateurs susceptibles d'avoir utilisé cette adresse à un moment donné.

- **Les données d'identification**

Sous cette rubrique, on trouve d'autres données comme par exemple :

- les identifiants pour accéder à des comptes bancaires ou des comptes chez des sites marchands sont attribués à une personne clairement identifiable (login) ;
- les identifications sous forme de pseudonymes, utilisées notamment pour les forums ou les blogs ou les adresses de messagerie, etc.

II.2.2. Des données transmises volontairement, ou à l'insu, de l'internaute

La plupart des données sont transmises volontairement et de manière transparente par l'utilisateur pour ses besoins de consultation de sites, de courriels, de recherches, d'achat,...

En revanche certaines données, notamment les données techniques, mais également des données comportementales sont transmises, voire conservées, à son insu (adresse IP, durée de communication, durée de consultation d'un site ou d'une de ses fenêtres, liste des sites consultés, voire mouvement de la souris, etc.).

L'utilisateur ne sait d'ailleurs pas à qui ces informations sont communiquées, même dans le cas où ces informations ont été volontairement transmises (FAI, hébergeur, responsable du site, voire partenaire du site ou sous-traitant spécialisé). Il faut noter que fréquemment les responsables de sites permettent à leurs partenaires et sous-traitants un accès à la communication de l'utilisateur de façon non transparente pour ce dernier.

II.2.3. Des données de contenu au statut divers

Enfin dans les grandes catégories de données transitant sur Internet il faut distinguer les données relevant de la correspondance privée comme les courriers électroniques des données de consommation, de comportement commercial ou social.

La diversité des données présentes sur le réseau constitue ainsi une mine de renseignements que certains acteurs cherchent à obtenir et capter pour des besoins extrêmement divers.

III. DES DONNEES UTILISEES PAR LES ACTEURS AU-DELA DE LA STRICTE NECESSITE DE LA COMMUNICATION DE LA CONSULTATION OU DE LA TRANSACTION

Une première motivation des acteurs de l'Internet, fournisseurs de services ou FAI, est de mieux connaître leurs utilisateurs ou clients afin d'optimiser les services rendus ou d'augmenter leur chiffre d'affaires, voire de les transmettre ou les revendre à des tiers : Il s'agit généralement de collecter le maximum d'informations à des fins de politique marketing. Une telle collecte d'informations n'est d'ailleurs pas spécifique au média Internet mais est grandement facilitée par celui-ci.

La seconde motivation, complémentaire de la première, est liée au modèle économique d'internet reposant pour un certain nombre de services sur la gratuité et la publicité. Dès lors, les annonceurs cherchent à obtenir un maximum d'informations pour effectuer des publicités les plus ciblées possibles et obtiennent de certains fournisseurs de services l'accès à des données qui ne leur étaient pas destinées.

Enfin, l'obtention d'informations peut être recherchée dans le but de nuire: recherche d'informations sur la vie privée, tentatives d'escroquerie, espionnage économique ou étatique...

En conséquence, bien que non quantifiés, l'échange et la revente d'informations obtenues au travers d'internet, correspondent à des flux financiers significatifs. A titre d'exemple, on estime le CA en France de la publicité internet à 2 Milliards d'€ (observatoire de la publicité), laquelle n'est qu'une partie des échanges financiers induits par cette activité.

IV. DES UTILISATIONS QUI POSENT PROBLEME AU REGARD DU RESPECT DE LA VIE PRIVEE

L'enregistrement direct ou indirect des données que l'internaute transmet à plusieurs acteurs de la chaîne de services (informations personnelles ou impersonnelles, sites consultés, contenu consulté à l'intérieur du site, durée, fréquence, mode de comportements) va souvent au-delà des nécessités de l'exploitation du service et peut constituer une atteinte au respect de la vie privée des internautes.

Cet enregistrement d'informations peut être réalisé soit directement par le fournisseur de service consulté ou par le FAI¹, soit par un tiers (société spécialisée ou autre fournisseur de service) auquel le fournisseur de service recherché a donné « la main » à l'insu de l'utilisateur.

On peut distinguer trois grandes catégories de situations qui méritent attention :

IV.1. La consolidation des données

Lors d'une visite sur un site d'information un internaute peut ne laisser que des traces anonymes. Cependant lorsqu'il achète un produit sur Internet son identité réelle est déclinée. Des sociétés spécialisées dans la consolidation de données, parviennent, dans les faits à l'identification réelle des internautes avec un profil de leurs habitudes et comportements extrêmement précis, même si certaines des données apparaissent anodines. Le but de ces

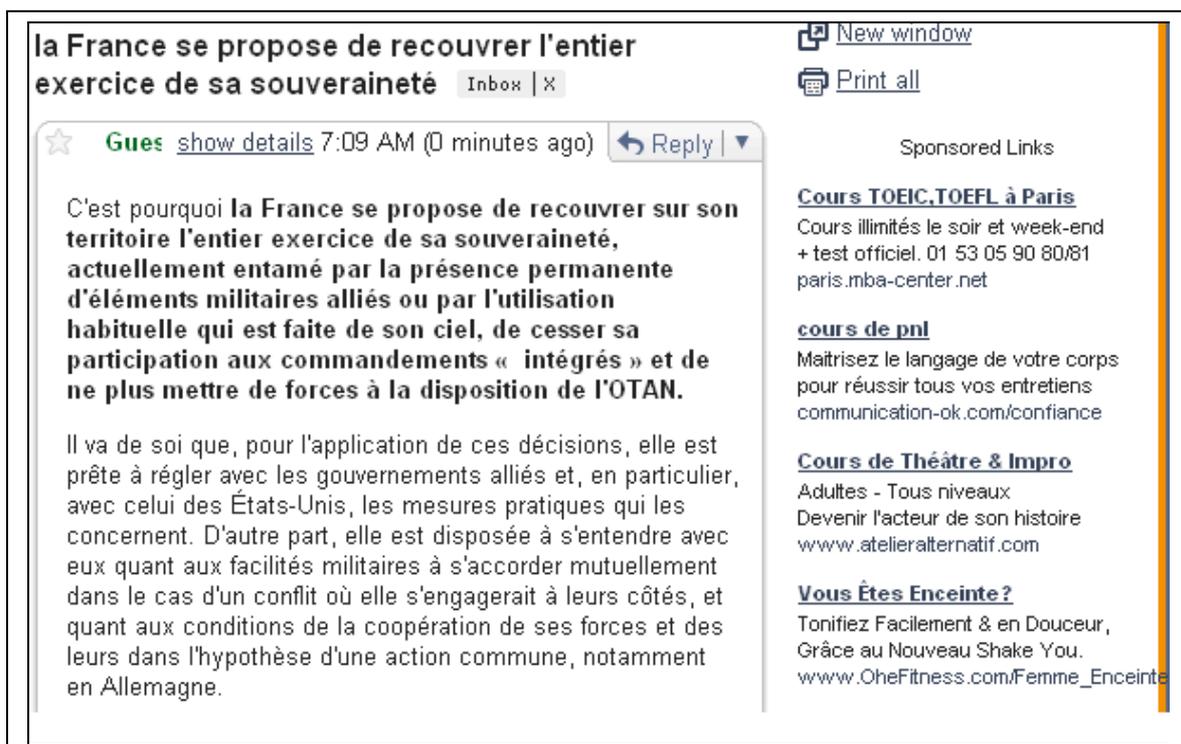
¹ à noter que l'enregistrement des données pour les FAI est encadré par le CPCE (Code des Postes et Communications Electroniques)

sociétés est de pouvoir pratiquer une publicité ciblée au mépris du respect de la vie privée des internautes qui n'ont pu en aucune façon être avertis, et encore moins consentir, du sort des données déposées par eux mêmes sur internet de façon dispersée.

IV.2. Les robots de messagerie

L'usage de robots de messagerie, qui analysent les messages transmis, semblent être devenus pratique courante. Ces robots cherchent des mots clés dans les messages transmis ou reçus pour mieux cerner le profil des internautes utilisant ces services. La plupart du temps ces messages agissent à l'insu des internautes.

La référence à ces pratiques dans les codes de déontologie de certains fournisseurs de messagerie ne règle d'ailleurs pas la question car si l'abonné à cette messagerie a pu lire les clauses du code de déontologie attaché à l'usage de cette adresse de messagerie, et donc savoir que les messages envoyés pourront être analysés, les internautes envoyant des messages à cette adresse n'ont aucune raison de connaître les règles de déontologie régissant l'adresse à laquelle ils envoient un message. Leur message se trouve donc analysé et scruté sans qu'ils aient pu avoir le moindre choix en la matière.



The screenshot shows a Gmail interface. The main message is titled "la France se propose de recouvrer l'entier exercice de sa souveraineté" and is from "Gues" sent at 7:09 AM. The message text discusses France's military presence and its stance on NATO. To the right, there are "Sponsored Links" for TOEIC courses, PNL courses, and theater/improvisation courses.

la France se propose de recouvrer l'entier exercice de sa souveraineté Inbox | X

☆ **Gues** [show details](#) 7:09 AM (0 minutes ago) Reply | ▼

C'est pourquoi **la France se propose de recouvrer sur son territoire l'entier exercice de sa souveraineté, actuellement entamé par la présence permanente d'éléments militaires alliés ou par l'utilisation habituelle qui est faite de son ciel, de cesser sa participation aux commandements « intégrés » et de ne plus mettre de forces à la disposition de l'OTAN.**

Il va de soi que, pour l'application de ces décisions, elle est prête à régler avec les gouvernements alliés et, en particulier, avec celui des États-Unis, les mesures pratiques qui les concernent. D'autre part, elle est disposée à s'entendre avec eux quant aux facilités militaires à s'accorder mutuellement dans le cas d'un conflit où elle s'engagerait à leurs côtés, et quant aux conditions de la coopération de ses forces et des leurs dans l'hypothèse d'une action commune, notamment en Allemagne.

New window
Print all

Sponsored Links

Cours TOEIC, TOEFL à Paris
Cours illimités le soir et week-end
+ test officiel. 01 53 05 90 80/81
paris.mba-center.net

cours de pnl
Maîtrisez le langage de votre corps
pour réussir tous vos entretiens
communication-ok.com/confiance

Cours de Théâtre & Impro
Adultes - Tous niveaux
Devenir l'acteur de son histoire
www.atelieralternatif.com

Vous Êtes Enceinte?
Tonifiez Facilement & en Douceur,
Grâce au Nouveau Shake You.
www.OheFitness.com/Femme_Enceinte

Exemple d'une boîte gmail. Il est clair que parfois les robots « ratissent large ». L'exemple ci-dessus est caricatural, puisqu'il évoque, au sujet du même courrier, un cours de langue étrangère, un cours de programmation, un cours de théâtre et une publicité féminine alors que courrier concerné parle de la place de la France dans l'OTAN. Et ils sont sans relation avec le destinataire ou avec l'expéditeur. Ceci est la preuve que les algorithmes nécessaires à la réelle maîtrise du Web sémantique ont encore des progrès à faire.

<p>Objet : [comptoir 171] Apple Shows Us DRM's True Colors</p> <p>Désolé de l'anglais, mais il dit bien ce que cela veut dire dans la langue de la petite pomme</p> <p>- le vrai rôle des DRM tant à l'honneur il y a peu <http://www.eff.org/deeplinks/2009/01/apple-shows-us-drms-true-colors></p> <p>- comme le vrai rôle de la Hadopi est sans doute ce que je disais cette semaine, de pouvoir :</p> <p>--- gérer les campagnes de promo dans le temps pour un meilleur impact commercial à moindre coût (piratage en produit d'appel) - pensez vous vraiment que je sois plus</p>	<p>Offre Limitée en Quantité à 99 €! www.Emailing-Network.com</p> <p>L Anglais vite pour Tous avec nos enseignants passionnés 01 42 66 04 32 et 0 800 200 140 www.businessstalkfrance.com</p> <p>Apprendre l'Anglais Formations et Perfectionnement pour Tous les Niveaux et à Distance www.cnfdi.com/cours_anglais</p> <p>Powerful DRM 90 Days FREE Control your digital media, ebook content Audio/Video, PDF, SWF Flash www.drm-x.com</p> <p>Probanse Direct Marketing Solution d'automatisation et de</p>
<p>Ici, le robot est beaucoup plus "efficace", puisque, partant d'un courriel bref, il propose, à partir de 3 mots clés du message, des propositions commerciales plausibles. Reste à savoir si l'utilisateur se sent concerné par ces messages et quel est le taux de clic. Information que Google ne donne évidemment pas.</p>	

Cf. également la recommandation 74-1 du rapport de la Commission parlementaire australienne en annexe 2 "Protecting a right to personal privacy".

IV.3. Les moyens techniques divers

Pour capter les données des internautes ou permettre de mieux cerner leur profil de consommateur ou de citoyen, plusieurs moyens sont utilisés, que ce soient des logiciels déposés sur l'ordinateur de l'utilisateur (cookies variés) ou des logiciels qui s'exécutent à l'extérieur et à l'intérieur de sa machine (scripts...) :

- **Les cookies** sont implantés par le fournisseur du service ou son sous-traitant sur la machine de l'utilisateur. Ils sont a priori un moyen de faciliter la connexion à un site fréquemment consulté. Mais au-delà de cette fonction, ils sont devenus un moyen d'enregistrement et de conservation de données diverses sur l'utilisateur « identifié » par sa machine. Les cookies « ordinaires » sont gérés par le navigateur de la machine de l'utilisateur et sont identifiables car déposés sur des fichiers déterminés. Leur fonction précise n'est pas déterminable par l'utilisateur ordinaire mais n'est accessible qu'à des amateurs éclairés ou des spécialistes. Ils peuvent être néanmoins facilement effaçables.

Site	Nom du cookie
voyages-sncf.com	s_sq
voyages-sncf.com	s_cc
voyages-sncf.com	sessionIdentificationLogin
voyages-sncf.com	VSCAuth
voyages-sncf.com	VSCPRDSession
voyages-sncf.com	RMFL
voyages-sncf.com	RMFD
voyages-sncf.com	RMPFW
voyages-sncf.com	tpid
voyages-sncf.com	s_vi
voyages-sncf.com	RMID
voyages-sncf.com	MC1
voyages-sncf.com	COOKIECHECK

Nom : sessionIdentificationLogin
Contenu : napoleon#Bonaparte
Domaine : .voyages-sncf.com
Chemin : /
Envoi pour : Tout type de connexion
Expire : lundi 26 avril 2077 23:56:16

Un cookie banal, ici gardant en mémoire (et en clair!) l'identifiant et le mot de passe d'un internaute. Ce site (voyages-sncf.com) implante 14 cookies, aux noms peu évocateurs de leur mission, sur l'ordinateur de l'internaute et les met à jour à chaque visite. Ici l'identifiant napoleon et le mot de passe "Bonaparte" sont séparés par un dièse.

A noter : la durée de validité de ce cookie, non paramétré par le webmestre, mais activé par le logiciel standard utilisé !

Site	Cookie Name
google.fr	
google.fr	__utma
google.fr	SID
google.fr	PREF
googleadservices.com	

Name: SID
Content: DQAAAHcAAADSg5i07pRpMmc6BQwKvE1QhsJNhbY1pM9k1H
Domain: .google.fr
Path: /
Send For: Any type of connection
Expires: mardi 6 juin 2017 14:42:30

Ici, Google ne donne pas non plus en clair le nom des champs (ici SID) et il en crypte le contenu et donc les informations d'identification de l'internaute qui visite son site, empêchant ainsi de connaître les données collectées à l'insu du visiteur.

A noter : la durée de validité de ce cookie.

- En revanche, d'autres types de cookies (exemple les cookies dits « adobe ») sont déposés sur les machines des internautes de manière nettement moins transparente et sont donc difficilement décelables et effaçables.
- **Les scripts** sont des logiciels s'exécutant en temps réel lors d'une connexion à un site afin de permettre a priori un meilleur « confort » de l'utilisateur dans sa consultation, mais au-delà de cette simple fonction, ils tendent à devenir un moyen privilégié d'affiner l'étude de comportement de l'utilisateur sur le site consulté.



Le lecteur « ordinaire » d'un quotidien en ligne (ici par exemple Libération) n'a pas accès aux accords donnés par le journal à un certain nombre d'autres acteurs (ici des agrégateurs de données) à venir observer son comportement, soit en déposant des cookies soit en activant des scripts sur la machine du lecteur.

Ici, grâce à un outil supplémentaire on prend connaissance des quatre sociétés concurrentes, qui profitent ainsi de cet accès pour glaner des infos sur le lecteur ou lui en offrir qui correspondent mieux à "son" profil.

Tout ceci à son insu, et sans que le journal, à aucun endroit, ne précise cette commercialisation du lecteur en échange des articles.

Dans aucun cas, il ne nous a été possible de connaître les accords contractuels et financiers entre l'éditeur et les agrégateurs.

```

function addDocLinksToSpan(xml, spanID)
{
    var span = document.getElementById(spanID);

    arts = xml.getElementsByTagName('article');
    for (i=0; i<arts.length;i++)
    {
        art = arts.item(i);
        var isFree = art.getAttribute('free');
        var titleArt =
art.childNodes[0].firstChild.nodeValue;
        var url = art.childNodes[1].firstChild.nodeValue;
        var newLink = document.createElement('a');
        newLink.className =
"texteRouge_tresPetitGras";
        span.appendChild(newLink);
        var text = document.createTextNode(titleArt);
        newLink.appendChild(text);
        newLink.href=url;
        text = document.createTextNode("\xA0");
        span.appendChild(text);
        if (isFree!="1")
        {
            var img =
document.createElement('img');
            img.src= monLibeBlanc;
            span.appendChild(img);
            text =
document.createTextNode("\xA0");
            span.appendChild(text);

        }
        var img = document.createElement('img');

        img.src= redBullet;
        span.appendChild(img);

        span.appendChild(document.createTextNode("\xA0"));
    }
}

```

Exemple: le début du script injecté par l'un de ces agrégateurs lorsqu'un internaute entre sur une page d'un quotidien.

Plutôt inoffensif, ce script-ci a pour objet d'afficher de la publicité contextuelle.

On notera néanmoins qu'il augmente singulièrement les volumes transmis dans les deux sens et ralentit ainsi les affichages de pages :

nous avons constaté dans certains cas qu'un dixième seulement du volume transmis est effectivement affiché sur l'écran de l'internaute.

Le reste des données sont des scripts effectuant ce back-office pour le compte des agrégateurs dans un cadre juridique gris !

- Enfin, il faut mentionner les « **spywares** » ou **logiciels espions**. Ceux-ci sont implantés à des fins frauduleuses ou criminelles² sur les machines des internautes mais la distinction avec les logiciels de ce type déposés à des fins « commerciales » est a priori mal déterminée, tant aux plans juridique que technique.

² La même technologie commence d'ailleurs à être utilisée, à des fins de surveillance fine (et donc non frauduleuse et criminelle) par les polices de certains pays. Le risque de l'extension de ces pratiques à des polices privées (les ayants droit de la musique les testent...) est néanmoins très préoccupant.

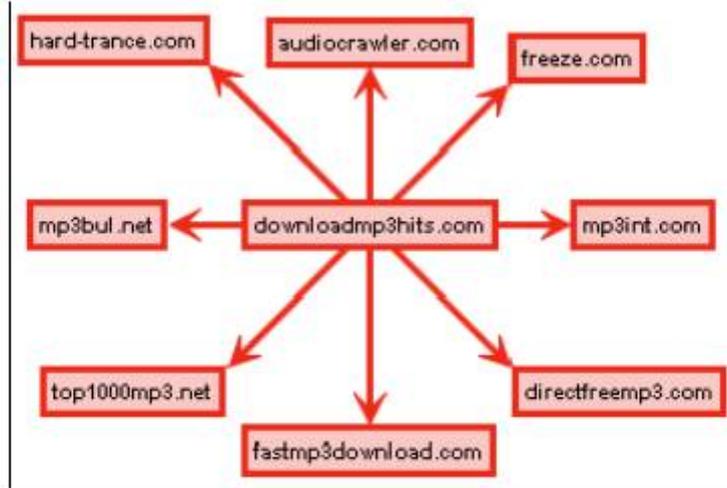
downloadmp3hits.com



D'après nos tests, ce site propose des liens pointant vers audiocrawler.com, une page qui a su déjouer le système de sécurité des navigateurs de notre ordinateur de test.

Ici, le site downloadmp3 est nocif, puisqu'il autorise un acteur tiers (audiocrawler) à modifier la configuration profonde de l'ordinateur.

Si l'internaute n'a pas d'outils d'alerte (tel celui utilisé ici) et de protection activés lors de ses visites, il est clair que le contrôle de son ordinateur ne lui appartient plus et qu'au pire, sa machine peut dorénavant être télécommandée à distance pour accomplir à son insu des actes malveillants et illégaux!



Ainsi ce site incitant au téléchargement (illégal ?) de musique est en fait une porte ouverte vers huit sites douteux, lesquels, bien entendu, restent cachés de l'utilisateur.

V. DES RISQUES FORTEMENT ACCRUS D'ATTEINTE A LA VIE PRIVEE DES UTILISATEURS

La capacité et la grande facilité des acteurs professionnels de l'internet à obtenir, voire à les capter à leur insu, des données sur leurs utilisateurs et leurs comportements accroît désormais les risques d'atteinte à la vie privée de ces derniers et ce à plusieurs niveaux.

V.1. Des données a priori impersonnelles peuvent aisément être personnalisées

La consolidation des données citée plus haut permet une personnalisation de données initialement impersonnelles au moins pour la plupart d'entre elles.

Les techniques de profilage à fins commerciales – pour ne citer qu'elles – permettent, par consolidation d'un certain nombre des informations captées, de dresser des profils relativement précis d'usage et de comportement des utilisateurs.

La mise en correspondance d'un profil déterminé, a priori impersonnel, avec une identité précise est aisément rendue possible du fait, qu'à un moment ou un autre lors de sa navigation sur internet, l'utilisateur fournit son identité réelle à un autre site consulté (site de vente en ligne par exemple,...). Cette mise en correspondance est d'autant plus probable qu'on assiste à une très grande concentration des sociétés spécialisées³ fournisseurs en outils de captage et de recueil de données pour le compte de fournisseurs de services internet (par exemple, un gestionnaire de scripts est généralement fournisseur de nombreux offreurs de services).

Ces sociétés spécialisées deviennent ainsi de plus en plus détentrices d'un grand nombre d'informations concernant des utilisateurs d'Internet identifiables ou identifiés et peuvent pratiquer des recoupements qui permettent in fine l'identification. Le risque d'atteinte à la vie privée, directement ou indirectement, est d'autant plus accru que ces profils de clients ont aujourd'hui une valeur marchande effective et sont l'objet, dès lors, d'un plus grand nombre d'échanges. De plus, un certain nombre de ces acteurs n'étant pas établis sur le territoire français, ou même européen, ne sont pas tenus de respecter la législation française ou européenne en matière de protection des données.

Il existe un facteur aggravant. Une fois le profil et le nom de l'internaute trouvés, surtout à son insu, la diffusion volontaire ou non, de ces informations personnelles, est irréversible et irrémédiable. Il en serait par exemple ainsi de la divulgation de la maladie chronique d'un internaute dont les assurances et l'entourage pourrait difficilement faire abstraction une fois qu'elles en auraient eu connaissance.

V.2. Des données nominatives insuffisamment protégées

L'analyse des messages transmis par des robots de messagerie à l'insu des usagers présente une atteinte inacceptable au respect de la vie privée et porte atteinte au secret de la correspondance.

³ Noms des sociétés : Doubleclick, Cybermonitor, Overture, SmartAdserver, Google-analytics, etc.

Ces robots procèdent par captation de mots présents dans les messages circulant sur internet et les informations ainsi recueillies, analysées, potentiellement diffusées et enregistrées sont utilisées pour « profiler » les comportements des utilisateurs. L'utilisation de ces outils ne fait pas toujours l'objet d'une autorisation préalable de l'utilisateur qui, dans la quasi totalité des cas, ne peut même pas concevoir l'existence de telles pratiques (les robots).

De même, le développement des réseaux sociaux et des blogs qui touche désormais des catégories de plus en plus jeunes pose le problème de l'utilisation actuelle ou à venir des données communiquées certes volontairement par les utilisateurs de ces sites mais recueillies par certaines sociétés voire conservées pour des durées plus ou moins longues⁴. Ce problème a d'autant plus d'acuité qu'encore une fois les acteurs professionnels peuvent être des sociétés non établies dans l'Union Européenne et donc non soumises à sa législation en matière de protection des données et de la vie privée.

Enfin, au travers d'entretiens qu'ont pu avoir les rapporteurs, il apparaît que la correspondance entre l'adresse IP anonyme et l'identité d'un abonné peut ne pas être toujours aussi bien protégée qu'elle devrait l'être et être relativement facilement accessible à des tiers autres que les fournisseurs d'accès Internet. (Ces derniers ne sont pas autorisés à les diffuser sauf aux autorités publiques dans les conditions légales et réglementaires prévues).

VI. DES PROTECTIONS RELATIVEMENT INSUFFISANTES FACE A CES RISQUES

VI.1. Des protections techniques individuelles mal connues voire limitées

Les internautes ne sont pas complètement sans défense face à cette intrusion dans leur vie privée mais les outils à leur disposition sont loin d'être suffisants ou satisfaisants.

Si la protection contre les virus et les logiciels espions est désormais accessible très largement par la commercialisation d'outils logiciels appropriés, il n'en est pas de même concernant les outils permettant potentiellement une meilleure protection de la vie privée comme par exemple les anonymiseurs. Ces outils relèvent plutôt du spécialiste ou de l'amateur éclairé que de l'utilisateur traditionnel. Ils ne font par ailleurs pas l'objet d'une large diffusion commerciale comme c'est le cas par exemple pour les anti-virus. En effet, ces outils de « discrétion » ont la particularité de faciliter tout autant les comportements délictueux (escroquerie, piratage,...). En tout état de cause, une certification internationale ou européenne de ceux-ci serait à étudier.

En outre, leur efficacité semble limitée sauf à se priver d'accès à un certain nombre de services internet.

⁴ Voir la tentative du site Facebook de février 2009 de modifier de façon drastique la propriété et l'utilisation des données personnelles de ses "membres". Le plus remarquable est que la communauté des internautes a réussi à modifier les décisions de Facebook en deux jours alors qu'aucune loi, dans aucun pays, ne peut avoir le même effet sur l'ensemble de la planète ni la même réactivité.

Il n'existe par ailleurs pas à notre connaissance d'outils techniques suffisamment puissants pour se prémunir totalement contre les consolidateurs de données, voire pour leur fournir des faux profils. Par ailleurs la cryptographie semble être le seul moyen pour lutter contre les violations des espions de messagerie, or celle-ci est contraignante et peu envisageable pour un usage courant, car la facilité d'usage va en sens opposé du niveau de protection.

Mp3 Gratuit

New: webradios gratuites Europe 2
100% Rock, sans pub, 24/24 et 7/7
www.europe2.fr

Tout sur Mp3 Gratuit

News, téléchargements, paroles
grâce à la toolbar Starware.
Musique.Starware.com

Mp3 Gratuit ✓

New: webradios gratuites Europe 2
100% Rock, sans pub, 24/24 et 7/7
www.europe2.fr

Tout sur Mp3 Gratuit ✗

News, téléchargements, paroles
grâce à la toolbar Starware.
Musique.Starware.com

A gauche la publicité telle que l'internaute la voit dans la majorité des cas. A droite, telle qu'il peut la voir s'il utilise des outils supplémentaires disponibles sur Internet (dont certains gratuits). Il est ainsi immédiatement alerté du caractère douteux du service offert par Starware (voir le détail du spyware ci-dessus). Et il en obtient un peu plus s'il positionne sa souris sur le feu vert ou rouge :

McAfee SiteAdvisor
Mp3 Gratuit
europe2.fr
We've tested this site and found no significant problems.

- ▶ 1 green download
- ▶ < 1 e-mail/ month
- ▶ Linked to green sites [More info...](#)

Try / buy other McAfee products

www.samsung.com

Mp3 Gratuit ✓
New: webradios gratuites Europe 2
100% Rock, sans pub, 24/24 et 7/7
www.europe2.fr

McAfee SiteAdvisor
Tout sur Mp3 Gratuit
starware.com
Use caution.

- ▶ 36 red downloads
- ▶ 1.2 e-mails/month
- ▶ Linked to green site [More info...](#)

Try / buy other McAfee products

www.europe2.fr

Tout sur Mp3 Gratuit ✗
News, téléchargements, paroles
grâce à la toolbar Starware.
Musique.Starware.com

puis en cliquant sur "more info" (exemple à droite):

DOWNLOAD TESTS FOR STARWARE.COM: ?

36 red downloads
In our tests, we found downloads on this site that some people consider adware, spyware, or other unwanted programs.

- ▶ [View detailed analysis](#)
- ▶ [Submit a download for analysis](#)
- ▶ [See how McAfee can protect your PC from dangerous downloads.](#)

Downloads we found on this site:

Download	Analysis
✗ auctions.exe	Adware-Cometsys
✗ buddies.exe	Adware-Cometsys
✗ entertainment.exe	Adware-Cometsys
✗ entertainment.exe	Adware-Cometsys
✗ horoscopes.exe	Adware-Cometsys

36 total downloads. [See more.](#)

VI.2. Une protection juridique insuffisante dans son application effective voire dans son champ

VI.2.1. Un encadrement juridique très générique

Pour la France, l'encadrement juridique des services internet est éclaté dans plusieurs textes couvrant des domaines a priori très différents :

- loi « informatique et liberté » n° 78-7 du 06-01-78,
- loi « Godfrain » (chapitre III) du 05-01-88,
- loi pour la confiance dans l'économie numérique n° 2004-57 du 01/06/04
- code des postes et communications électroniques (CPCE).

La loi "informatique et liberté" a pour objectif la protection de la vie privée dans l'environnement informatique. A ce titre elle émet des obligations concernant les entités responsables de fichiers et de données informatiques (article 32, en annexe 3) qui prévoient une utilisation loyale des données recueillies et en parallèle le droit à l'information des personnes concernées. Celles-ci ont également un pouvoir d'opposition et de correction vis-à-vis de ces données. La durée de conservation des données est également encadrée. Compte tenu de ce champ d'application elle couvre également les données liées aux services internet.

La "loi Godfrain", pour sa part, a pour objectif de sanctionner les attaques frauduleuses ou criminelles de systèmes informatiques installés sur le territoire français. Elle ne prend pas en compte les abus possibles en matière commerciale mais elle trouve également son application dans le domaine Internet dans les cas de dispositifs d'intrusion comme les « spyware » par exemple (annexe 4).

La loi pour la confiance dans l'économie numérique a pour objectif principal d'établir les règles et responsabilités respectives concernant les hébergeurs, les éditeurs de sites et le e-commerce. Elle est essentiellement tournée vers l'irresponsabilité a priori des hébergeurs pour le contenu qu'ils hébergent et la protection du consommateur dans le e-commerce. Les préoccupations de respect de la vie privée ne sont pas intégrées dans ce texte.

Le CPCE, a pour objectif principal d'édicter les règles régissant les opérateurs de communications électroniques, dont font partie les fournisseurs d'accès à Internet. Sur le plan du respect de la vie privée, il a pour dispositions principales :

- le respect du secret des correspondances, qui s'applique aux communications téléphoniques mais également aux courriels (article L34,...) ;
- l'encadrement de la conservation des données qui consiste en une obligation de destruction des données recueillies à l'exception de certains cas prévus par la loi article L34-1-1, annexe 5) ;
- l'interdiction des spams ou messages non sollicités (L 34-5 & R 10 sq.) ;
- l'interdiction d'utiliser les données recueillies sur leurs abonnés par les opérateurs de communications électroniques à l'exception de leurs besoins propres et avec consentement exprès de l'abonné(R 34-1 III).

Il est à noter que le code ne vise pas les fournisseurs de services de communications au public en ligne (fournisseurs de contenus- éditeurs).

Le législateur a ainsi mis en place un dispositif qui peut sembler suffisant et complet. Toutefois la nature souvent trop générale des dispositions prises ou à l'inverse le champ d'application restreint à certains acteurs ne permet d'avoir un corpus juridique suffisamment protecteur concernant l'ensemble des particularités d'Internet. La plupart de ces textes ont été adoptés soit avant qu'internet n'existe soit avant sa diffusion massive ce qui les rend parfois inopérants et souvent imprécis, ceci pouvant d'ailleurs s'avérer un atout dans certains cas.

Par exemple le droit à l'information de l'internaute sur l'utilisation qui sera faite de ses données est un principe général nécessaire qui peut couvrir de nombreux cas de figure. Toutefois son application n'est pas facilement adaptable aux différentes situations actuellement rencontrées par les internautes : renvoi en cascade entre fournisseur de services, recours généralisé à des sous-traitants spécialisés..., car aucune règle d'application plus précise n'est édictée permettant de guider les acteurs de l'Internet d'une part et de fournir un fondement plus précis aux éventuels recours des internautes.

S'agissant du secret des correspondances, celui-ci est protégé largement et énergiquement par le CPCE ou le code pénal. Toutefois ce principe général n'est pas décliné spécifiquement pour internet et ne vise donc pas expressément l'usage qui peut être fait des robots de messagerie. Or leur activité se trouve à la frange du secret des correspondances et le silence des textes se prête aux interprétations non favorables au respect de la vie privée.

VI.2.2. Des moyens de contrôle peu développés ou inadaptés

Au-delà de l'insuffisance du champ d'application de la législation, la question du contrôle de son application se pose pour lui donner une véritable efficacité.

Qu'il s'agisse des FAI ou des fournisseurs de services les moyens dévolus à cette tâche sont peu développés voire inexistants. Les moyens de la CNIL, par exemple, ne sont pas toujours à la hauteur des enjeux dans la mesure où le développement constant d'internet, tant par le nombre d'abonnés que par le nombre de sites, a créé un secteur entièrement nouveau par rapport aux missions qui étaient déjà dévolues à la CNIL.

Les FAI, pour leur part, sont soumis au contrôle de l'ARCEP ou des agents du ministère chargé des communications électroniques. Ce contrôle concerne notamment les données qu'ils recueillent au titre des services d'abonnement qu'ils offrent.

En outre, d'une façon générale le niveau des sanctions financières qui peuvent être édictées dans le cadre de la législation actuelle (CNIL, loi Godfrain,...) est insuffisamment dissuasif par rapport à la taille de certains acteurs internationaux.

Toutefois compte tenu de la sensibilité de l'opinion publique à la question du respect de la vie privée, les acteurs eux-mêmes font des tentatives pour édicter des règles de bonne conduite par le biais de codes de déontologies ou de conditions générales de vente incluant ces préoccupations. C'est notamment le cas des grandes sociétés aux Etats-Unis où l'opinion publique est sensibilisée à ces questions.

Ces textes constituent un premier pas et semblent marquer une bonne volonté des acteurs mais souffrent d'un caractère parfois imprécis et ambigu, voire entérinent certaines pratiques contestables (utilisation de robots de messagerie par exemple). Par ailleurs, émanant le plus souvent de sociétés étrangères, ces textes sont calés sur le droit de leur propre pays plus que sur les pratiques européennes et françaises et n'apportent pas obligatoirement les réponses espérées. Enfin ces textes n'ont pas de valeur juridique contraignante mais sont seulement une liste de bonnes intentions dont la non-réalisation n'est pas sanctionnable.

Le respect de la vie privée dans l'usage d'internet n'est pas une préoccupation spécialement française ni même européenne mais est un sujet d'inquiétude pour de nombreux pays où des réflexions sont engagées. L'Australie, par exemple, est avancée en la matière : le rapport d'août 2008 présenté par la commission des lois australiennes, faisant suite à une vaste enquête englobant tous les aspects de la vie privée et qui propose une réforme globale de la législation, montre l'universalité de cette préoccupation.

De plus la présence de nombreuses sociétés implantées hors du territoire national, pose un véritable problème d'efficacité de la législation puisque ces entreprises peuvent, dans bien des cas, se prétendre hors d'atteinte des règles que l'on voudrait leur imposer. Les efforts déployés par le groupe de l'article 29 qui réunit les offices de protection des libertés européen du type CNIL montrent que cette préoccupation grandissante est largement partagée. La XXX^{ième} conférence mondiale des commissaires à la protection des données et à la vie privée vient de charger un groupe de travail pour effectuer une proposition commune d'établissement de normes internationales sur la vie privée et la protection des données personnelles (article 3 d'une résolution d'octobre 2008) (annexe 6).

B - PISTES DE PROPOSITIONS A APPROFONDIR

Face à ces risques importants de dérive, qui tendent à se concrétiser dès à présent dans le domaine de la consolidation des données et de la correspondance privée deux axes de propositions peuvent être esquissés pour s'assurer d'une protection plus effective du respect de la vie privée des internautes : affirmation d'un véritable droit à l'anonymat, obligation de transparence/droit de savoir ce qui me concerne et renforcement du secret des correspondances, dans les deux dimensions indissociables juridique et technique.

VII. L’AFFIRMATION D’UN VERITABLE DROIT A L’ANONYMAT ET DROIT DE SAVOIR

Cette proposition peut se décliner sous plusieurs formes selon les services utilisés.

VII.1. Cas de la consultation d'un site

Si l'identification réelle (nom, coordonnées) est nécessaire pour accéder au service recherché.

Quatre cas d'autorisations devraient être explicitement proposés par le fournisseur de service :

- accord pour donner ses données dans la seule utilisation en cours sans possibilité de les transmettre ou de les conserver ;
- accord pour une utilisation générique de ses données pour le seul fournisseur de contenus consulté ;
- accord pour une diffusion à une liste limitée de bénéficiaires (par exemple le fournisseur de contenu, mais aussi les parties prenantes sur le dossier) ;
- accord pour diffuser ses données à tous.

Enfin une proposition systématique d'anonymisation des données fournies, qui permet alors une utilisation des données anonymisées, devrait être également prévue.

Cette segmentation devrait être rendue obligatoire pour les sites des fournisseurs de service établis en France et sanctionnée en cas de manquement. Elle ne peut être étendue dans l'état actuel du droit à l'ensemble des sites consultés par les français mais implantés à l'étranger. Cette mesure même ainsi limitée aurait un impact réel dans la mesure où les sites consultés depuis la France et exploités par des fournisseurs de service établis sur le territoire national représentent l'essentiel du trafic. C'est ainsi que parmi les 30 sites les plus consultés par les français, plus de la moitié sont des sites français (source Médiamétrie, en annexe 7), ce chiffre intégrant les moteurs de recherche. Le respect de la loi française par ces sites installés en France peut être un avantage compétitif pour eux car ils pourront mettre en avant les précautions prises, et contrôlées sous peine de sanction, ce que peut difficilement faire un site installé à l'étranger.

Toutefois une réflexion au niveau européen pour étendre cette mesure à l'ensemble des fournisseurs de service de l'Europe devrait être engagée.

Piste 1 : Affirmer un véritable droit à l'anonymat numérique et de transparence sur l'usage fait des données individuelles.

Piste 1-1 : introduction d'autorisations explicites graduées et passibles de sanctions pour l'utilisation des données personnelles d'identification.

VII.2. Cas des consolidateurs de données

Il est nécessaire de prévoir des mesures permettant à l'internaute de rester maître de ses données dans le temps, notamment si elles sont nominatives.

Il ne s'agit pas de s'opposer à l'activité des consolidateurs de données dès lors que les données ont été communiquées de façon volontaire. Ce serait aller contre le principe de la liberté du commerce et de l'industrie et mettrait en péril le modèle fondé sur la publicité. Pour autant l'activité et les moyens de l'exercer par ces sociétés devrait faire l'objet d'une attention des pouvoirs publics.

Si les précautions préconisées ci-dessus pour obtenir l'accord explicite de l'abonné sont en place, la consolidation de données ne concernera plus que des internautes consentants. Toutefois la durée de ce consentement ne doit pas être considérée comme éternelle. Les données ainsi recueillies doivent donc être effacées automatiquement, ou anonymisées, après un délai inférieur ou égal à 1 an, à l'exemple de l'accord intervenu entre la CNIL et les moteurs de recherche.

La législation en la matière semble suffisante, au moins pour ce qui concerne les activités soumises à la législation française, sous réserve éventuellement d'une aggravation des sanctions en cas de manquement. Toutefois au-delà des textes, les difficultés sont nombreuses du fait que les sociétés consolidatrices sont le plus souvent situées hors du territoire national et n'ont pas besoin d'avoir un établissement en France pour exercer leur activité. Une piste de réflexion pour pallier ce problème pourrait être d'imposer des clauses obligatoires prévoyant ce type de dispositions d'effacement ou d'anonymisation dans les contrats passés entre les fournisseurs de service français et les consolidateurs de données. Un pouvoir de vérification des ces clauses contractuelles serait conféré à la DGCCRF dans le cadre de la protection des consommateurs.

Piste 1-2 : introduire l'obligation d'effacement des données personnelles dans les contrats que les fournisseurs français de services internet passent avec les consolidateurs de données.

VII.3. Cas des gestionnaires d'identifiants personnels

Il est, là aussi, nécessaire de prévoir des mesures permettant à l'internaute de rester maître de ses données dans le temps, d'autant plus qu'elles sont nominatives et souvent sensibles (ex : données médicales avec le DMP, Dossier médical personnalisé) et il serait également nécessaire que les autorités puissent s'assurer que ces données sont stockées de façon sécurisée et ne sont pas soumises à des utilisations autres que celles prévues par les

cahiers des charges et les contrats. Alors que certains opérateurs disent stocker les informations personnelles des internautes français à l'extérieur des frontières européennes (cf. la charte de Yahoo en annexe 8), il apparaît primordial que les données sensibles des citoyens français puissent être placées sous l'autorité de la loi nationale. Cela pourrait passer par un véritable statut juridique des données personnelles, précisant les droits et obligations des parties prenantes. Ce statut devrait être décliné selon les grands secteurs car les règles imposées aux données bancaires ne doivent pas forcément être les mêmes que celles imposées aux données médicales par exemple. Par ailleurs dans ce cadre les droits et obligations des personnes physiques « détentrices » des données personnelles ne doivent pas être les mêmes que ceux des professionnels de ces secteurs qui les recueillent et les utilisent.

De tels statuts devraient être étendus au niveau européen.

Piste 1-3 : définition de statuts pour les données personnelles (exemple du DMP) et les identifiants personnels.

VII.4. Cas des FAI

Les FAI sont soumis aux règles du CPCE et à ce titre sont soumis au secret des correspondances. Par ailleurs l'utilisation des données qu'ils recueillent ainsi que leur conservation sont encadrées par le code dans ses articles L34 et suivants, avec des sanctions pénales possibles (L39-1).

La levée de l'anonymat par rapprochement de l'adresse IP et du nom de leurs abonnés auxquels l'adresse a été attribuée à un instant donné est interdite sur le principe par la CNIL (traitement de données) et le CPCE qui limite l'usage des données ainsi recueillies aux seules exigences de l'autorité judiciaire ou administrative prévues par la loi. Dans ces conditions il serait sans doute nécessaire que les FAI sensibilisent leur personnel à cette interdiction et leur rappellent les sanctions encourues par l'entreprise, et l'éventuelle responsabilité qui pèserait sur le personnel ayant contrevenu à cette obligation. Par ailleurs, les FAI devraient faire la preuve que toutes les mesures de sécurité sont prises dans leur organisation interne pour le respect de leurs obligations et des moyens de contrôle externe devraient être développés.

Piste 1-4 : Rappeler aux opérateurs leur responsabilité face aux libertés que leurs personnels prennent parfois avec leurs obligations de secret professionnel malgré les sanctions prévues.

VIII. LE RESPECT DU SECRET DES CORRESPONDANCES : CAS DES ROBOTS DE MESSAGERIE

Concernant les robots de messagerie, ceux-ci devraient voir leur utilisation sévèrement contrôlée, voire interdite. L'argument avancé qu'il s'agit de machines et non d'humains qui « auscultent » les communications (cf. la réponse de Google)⁵ ne semble pas très pertinent. Il s'agit ni plus ni moins que de la violation du secret des correspondances garanti par la loi même s'il ne s'agit pas d'interception proprement dite.

⁵ Annexes 9 et 9bis

Actuellement l'utilisation de ces robots n'est pas déclarée auprès des utilisateurs de la messagerie et il n'est donc pas possible à l'internaute de donner ou refuser son accord. Par ailleurs l'existence de messages entrants et sortants rend très complexe la généralisation d'un accord préalable efficace.

Or l'utilisation de ces robots même si elle est anonyme est une façon de récolter et conserver des données et doit obéir au même principe de transparence que toute collecte de données. Il serait donc utile de renforcer l'arsenal législatif pour obliger les robots, soit a minima à être déclarés, soit de préférence à être interdits.

Les robots qui recueilleraient des données non anonymes devraient être clairement hors la loi et assimilés à des interceptions illégales.

Cette question est loin d'être anodine dans la mesure où certains grands acteurs de l'Internet y font une référence quasi- explicite dans leur documentation.

Piste 2 : introduire dans la législation l'interdiction de l'usage des robots et automates collectant des données personnelles dans les courriels

IX. AUTRES DISPOSITIONS COMPLEMENTAIRES POUVANT ETRE ENVISAGEES

IX.1. Organiser le contrôle- application de la législation et de la réglementation, conformité des chartes de déontologie

Compte tenu des difficultés d'interprétation qui peuvent naître du caractère générique de certains textes, une concertation des différents acteurs publics (DGCIS, DGCCRF, CNIL, etc.) devrait permettre de faire une description précise et pratique des comportements et pratiques du monde de l'Internet qui tombent sous le coup des dispositions législatives et réglementaires. Une telle description donnerait un cadre de référence précis aux différents acteurs professionnels voire leur permettrait d'adapter leur comportement.

Une fois ce cadre bien précisé, il serait recommandé que la CNIL dans le cadre des pouvoirs d'enquête qui lui sont conférés lance une enquête sur la régularité des comportements et pratiques des différents acteurs situés sur le territoire national. A cet égard la CNIL devrait disposer des moyens suffisants pour effectuer des vérifications de cette nature, voire constituer une entité spécifique comme a pu le faire par exemple la DGCCRF à Morlaix pour la protection des consommateurs. Par ailleurs le niveau général des sanctions devrait être relevé pour être véritablement dissuasif face à des acteurs importants.

Piste 3-1 : Renforcer les vérifications et les sanctions en matière de protection des données personnelles par la CNIL, voire par un service de l'Etat.

IX.2. Etudier la faisabilité d'un label de bonne conduite en matière de respect de la vie privée pour les prestataires de services

Plusieurs ministères et entités (syndicats professionnels, Forum des droits de l'internet, etc.) pilotent et attribuent divers labels propres à la sphère internet. La visibilité et le suivi laissent à désirer. De plus, le respect de la vie privée et des données personnelles est mal encadré.

Il est ainsi proposé qu'un organisme (le futur CNN – Conseil National du Numérique – ou la CNIL) organise la mise en place d'un label avec la profession. Ce label permettrait d'aller au-delà du simple respect des pratiques légales sur le territoire national par les acteurs de l'Internet. Il certifierait que le détenteur du label exige également le respect de la vie privée des utilisateurs dans ses relations avec ses partenaires étrangers (non astreints à la législation française ou européenne) par des clauses contractuelles vérifiables.

Piste 3-2 : Clarifier, simplifier les régimes des labels relatifs à la vie privée sur Internet en France et en confier le pilotage à un seul organisme, par exemple la CNIL.

IX.3. Renforcer l'information des utilisateurs

L'information sur les pratiques existantes et potentielles et une sensibilisation sur les risques qui en découlent pour les internautes devrait être améliorée.

La CNIL a, sur ses propres supports, donné un certain nombre d'informations pour sensibiliser les internautes et a mis en place des campagnes d'information sur la protection des mineurs dans le cadre de la diffusion des réseaux sociaux. Ces actions constituent un effort réel et nécessaire mais demeurent encore incomplètes dans la mesure où elles n'abordent pas l'ensemble des problèmes mais se focalisent sur un public spécifique.

Compte tenu de la faible information des consommateurs en général, de l'insouciance des jeunes face à ces questions, du caractère parfois difficilement appréhendable par des internautes moyennement avertis de ces pratiques, de véritables campagnes publiques de sensibilisation devraient être effectuées à l'initiative des ministères concernés (consommation, famille, intérieur, etc.) sur l'ensemble des risques encourus et des moyens de se protéger.

Au-delà de cette information institutionnelle, les acteurs du secteur devraient participer à ce souci d'information par les moyens qui leur sont propres, cette action pouvant éventuellement devenir une de leurs obligations juridiques. Par exemple, on pourrait envisager la mise en place systématique, à chaque connexion d'un bandeau informatif énonçant les risques et les moyens de protection relatifs à la vie privée.

Piste 3-3 : Donner à la CNIL ou à une entité de l'Etat les moyens d'informer concrètement les utilisateurs des avantages, mais aussi des risques de l'usage des outils numériques.

Enfin, de même que l'intégrité et la sécurité des ordinateurs personnels sont (plus ou moins) protégés par des logiciels de veille et de barrages (les murs anti-feu), il nous paraît que le moment est maintenant venu de faire étudier et développer des logiciels paramétrables qui permettraient d'alerter l'internautes systématiquement lorsqu'un script cherche à capturer des données personnelles, nominatives ou non, mais sensibles. Un concours pourrait être organisé par la DGCIS pour tester des démonstrateurs d'un mur anti-feu des données privées de l'internaute.

Piste 3-4 : Faire organiser, par la DGCIS par exemple, un concours pour créer le mur anti-feu des données personnelles propres à chaque internaute.

Les propositions ci-dessus constituent une première réponse aux dérives observées qui permettrait une amélioration substantielle de la situation actuelle.

Il n'en reste pas moins qu'un renforcement de l'efficacité de ces mesures passe par la mise en place d'une législation européenne élargie pour couvrir l'ensemble de ces questions.

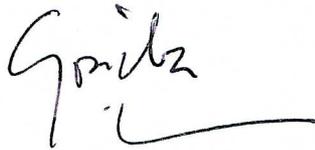
La France pourrait soutenir activement toute initiative de proposition de directive européenne ayant pour objet d'améliorer le respect de la vie privée des internautes en obligeant les acteurs établis sur le territoire européen à respecter des normes en la matière y compris dans leurs relations avec des acteurs étrangers.

Par ailleurs une véritable coopération internationale sur le sujet devrait s'établir à l'instar de ce qu'a entrepris le groupe de l'article 29 qui regroupe les organismes européens de protection des données.

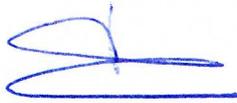
Piste 3-5 : Encourager l'Europe à renforcer les obligations qui devraient peser sur les acteurs en matière de recueil et d'exploitation de données personnelles.

* * * * *

Les rapporteurs,



J.C. GORICHON



D. VARENNE



M. SPORTICHE



**Conseil Général de l'Industrie,
de l'Énergie et des Technologies**

Internet et le respect de la vie privée

ANNEXES

RAPPORT N° IV-1.9-2008 – Mars 2009

Liste des annexes

- Annexe 1 : Liste des organismes rencontrés**
- Annexe 2 : Extrait "Australian Privacy Law and Practice"**
- Annexe 3 : Article 32, Loi "Informatique et Libertés" 78-7**
- Annexe 4 : Chapitre III, loi Godfrain du 05-01-88**
- Annexe 5 : CPCE, article L34-1**
- Annexe 6 : 30^e conférence Groupe "Article 29"**
- Annexe 7 : Fréquentation des sites Internet français (Médiamétrie)**
- Annexe 8 : Extrait charte "Données personnelles" de Yahoo**
- Annexe 9 : Extrait SVM "Google en sait-il trop sur vous?"**
- Annexe 9bis : Revue de presse Ministère: "Google et la vie privée"**

Organismes rencontrés

- Organisation « Que Choisir »,
- Association « Familles rurales »,
- ADEIC (Association de défense, d'éducation et d'information du consommateur),
- Yahoo France,
- ASK France,
- ACSEL,
- Price-Minister,
- La CNIL.

- (a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth);
- (b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and
- (c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

Recommendation 73–11 The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish educational material that addresses the:

- (a) rules regulating privacy in the telecommunications industry; and
- (b) various bodies that are able to deal with a telecommunications privacy complaint, and how to make a complaint to those bodies.

Part K—Protection of a Right to Personal Privacy

74. Protecting a Right to Personal Privacy

Recommendation 74–1 Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, a serious invasion of privacy may occur where:

- (a) there has been an interference with an individual's home or family life;
- (b) an individual has been subjected to unauthorised surveillance;
- (c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or
- (d) sensitive facts relating to an individual's private life have been disclosed.

Recommendation 74–2 Federal legislation should provide that, for the purpose of establishing liability under the statutory cause of action for invasion of privacy, a claimant must show that in the circumstances:

- (a) there is a reasonable expectation of privacy; and

Annexe 3

relation avec d'autres traitements ;

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en oeuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

II. - Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la commission :

- de tout changement affectant les informations mentionnées au I ;

- de toute suppression du traitement.

Article 31 En savoir plus sur cet article...

Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004

I. - La commission met à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26.

Cette liste précise pour chacun de ces traitements :

1° L'acte décidant la création du traitement ou la date de la déclaration de ce traitement ;

2° La dénomination et la finalité du traitement ;

3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celles de son représentant ;

4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ;

5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ;

6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

II. - La commission tient à la disposition du public ses avis, décisions ou recommandations.

III. - La Commission nationale de l'informatique et des libertés publie la liste des Etats dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.

▶ **Chapitre IV : Collecte, enregistrement et conservation des informations nominatives. (abrogé)**

Article 29-1 (abrogé) En savoir plus sur cet article...

Créé par Loi n°2000-321 du 12 avril 2000 - art. 5 JORF 13 avril 2000

Abrogé par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004

Article 33-1 (abrogé) En savoir plus sur cet article...

Créé par Loi n°2000-321 du 12 avril 2000 - art. 5 JORF 13 avril 2000

Abrogé par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

▶ **Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes**

▶ **Section 1 : Obligations incombant aux responsables de traitements.**

Article 32 En savoir plus sur cet article...

Créé par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

- 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
- 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
- 3° Du caractère obligatoire ou facultatif des réponses ;
- 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
- 5° Des destinataires ou catégories de destinataires des données ;
- 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;
- 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

II. - Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- des moyens dont elle dispose pour s'y opposer.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

III. - Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

IV. - Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

V. - Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

VI. - Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Article 33 En savoir plus sur cet article...

Modifié par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies.

Article 34 En savoir plus sur cet article...

Modifié par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Article 35 En savoir plus sur cet article...

Modifié par Loi n°2004-801 du 6 août 2004 - art. 5 JORF 7 août 2004

« Art. 23-6-1. - Les litiges nés de l'application de l'article 23-6 sont soumis à une commission départementale de conciliation composée de bailleurs et de locataires en nombre égal et de personnes qualifiées. La commission s'efforce de concilier les parties et rend un avis.

« Si le juge est saisi parallèlement à la commission compétente par l'une ou l'autre des parties, il ne peut statuer tant que l'avis de la commission n'est pas rendu.

« La commission est dessaisie si elle n'a pas statué dans un délai de trois mois.

« La composition de la commission, le mode de désignation de ses membres et ses règles de fonctionnement sont fixés par décret. »

Art. 3. - Après le sixième alinéa (5^o) de l'article 2 du décret n° 53-960 du 30 septembre 1953 précité, il est inséré un 6^o ainsi rédigé :

« 6^o Aux baux des locaux consentis à des artistes admis à cotiser à la caisse de sécurité sociale de la maison des artistes et reconnus auteurs d'œuvres graphiques et plastiques, tels que définis par l'article 7 de l'annexe III du code général des impôts. »

Art. 4. - Les dispositions de l'article 1^{er} de la présente loi sont applicables à compter du 1^{er} janvier 1988.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 5 janvier 1988.

FRANÇOIS MITTERRAND

Par le Président de la République :

Le Premier ministre,
JACQUES CHIRAC

Le ministre d'Etat, ministre de l'économie,
des finances et de la privatisation,
ÉDOUARD BALLADUR

Le garde des sceaux, ministre de la justice,
ALBIN CHALANDON

Le ministre de l'intérieur,
CHARLES PASQUA

Le ministre délégué auprès du ministre de l'économie,
des finances et de la privatisation,
chargé du commerce, de l'artisanat et des services,
GEORGES CHAVANES

Le ministre délégué auprès du ministre de l'intérieur,
chargé des collectivités locales,
YVES GALLAND

(1) Travaux préparatoires : loi n° 88-18.

Sénat :

Projet de loi n° 100 (1987-1988) ;

Rapport de M. Laurin, au nom de la commission des lois, n° 125 (1987-1988) ;

Discussion et adoption, après déclaration d'urgence, le 8 décembre 1987.

Assemblée nationale :

Projet de loi, adopté par le Sénat, n° 1109 ;

Rapport de M. Delattre, au nom de la commission des lois, n° 1145 ;

Discussion et adoption le 21 décembre 1987.

Sénat :

Projet de loi, modifié par l'Assemblée nationale, n° 205 (1987-1988) ;

Rapport de M. Laurin, au nom de la commission des lois, n° 213 (1987-1988) ;

Discussion et adoption le 22 décembre 1987.

**LOI n° 88-19 du 5 janvier 1988
relative à la fraude informatique (1)**

NOR : JUSX8700198L

L'Assemblée nationale et le Sénat ont adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Article unique. - Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

« Chapitre III

« De certaines infractions en matière informatique

« Art. 462-2. - Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces deux peines.

« Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10 000 F à 100 000 F.

« Art. 462-3. - Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines.

« Art. 462-4. - Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2 000 F à 500 000 F ou de l'une de ces deux peines.

« Art. 462-5. - Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 2 000 000 F.

« Art. 462-6. - Quiconque aura sciemment fait usage de documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 2 000 000 F ou de l'une de ces deux peines.

« Art. 462-7. - La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

« Art. 462-8. - Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

« Art. 462-9. - Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre. »

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 5 janvier 1988.

FRANÇOIS MITTERRAND

Par le Président de la République :

Le Premier ministre,
JACQUES CHIRAC

Le garde des sceaux, ministre de la justice,
ALBIN CHALANDON

(1) Travaux préparatoires : loi n° 88-19.

Assemblée nationale :

Proposition de loi n° 352 ;

Rapport de M. André, au nom de la commission des lois, n° 744 ;

Discussion et adoption le 15 juin 1987.

Sénat :

Proposition de loi, adoptée par l'Assemblée nationale en première lecture, n° 279 (1986-1987) ;

Rapport de M. Thyraud, au nom de la commission des lois, n° 3 (1987-1988) ;

Discussion et adoption le 4 novembre 1987.

Assemblée nationale :

Proposition de loi, modifiée par le Sénat en première lecture, n° 1009 ;

Rapport de M. André, au nom de la commission des lois, n° 1087 ;

Discussion et adoption le 21 décembre 1987.

Sénat :

Proposition de loi, adoptée avec modifications par l'Assemblée nationale en deuxième lecture, n° 212 (1987-1988) ;

Rapport de M. Thyraud, au nom de la commission des lois, n° 214 (1987-1988) ;

Discussion et adoption le 22 décembre 1987.

Assemblée nationale :

Proposition de loi, modifiée par le Sénat en deuxième lecture, n° 1182 ;

Rapport de M. André, au nom de la commission des lois, n° 1184 ;

Discussion et adoption le 22 décembre 1987.



Code des postes et des communications électroniques

Version consolidée au 19 février 2009

Partie législative

LIVRE II : Les communications électroniques

TITRE Ier : Dispositions générales

Chapitre II : Régime juridique.

Section 3 : Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques.

Article L34-1 En savoir plus sur cet article...

Modifié par Loi n°2006-64 du 23 janvier 2006 - art. 5 JORF 24 janvier 2006

I. - Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des II, III, IV et V.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.

III. - Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement les catégories de données techniques qui sont déterminées, dans les limites fixées par le V, selon l'activité des opérateurs et la nature de la communication, par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

Les opérateurs peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

IV. - Sans préjudice des dispositions du II et du III et sous réserve des nécessités des enquêtes judiciaires, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

V. - Les données conservées et traitées dans les conditions définies aux II, III et IV portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Article L34-1-1 En savoir plus sur cet article...

Créé par Loi n°2006-64 du 23 janvier 2006 - art. 6 JORF 24 janvier 2006

Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.

Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière.

Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.

Cette instance peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques. Lorsqu'elle constate un manquement aux règles définies par le présent article ou une atteinte aux droits et libertés, elle saisit le ministre de l'intérieur d'une recommandation. Celui-ci lui fait connaître dans un délai de quinze jours les mesures qu'il a prises pour remédier aux manquements constatés.

Les modalités d'application des dispositions du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises.

NOTA:

Loi n° 2006-64 du 23 janvier 2006 article 6 I : La présente version de cet article est en vigueur jusqu'au 31 décembre 2008.

Loi n° 2008-1245 du 1er décembre 2008 : les dispositions de l'article 32 de la loi n° 2006-64 du 23 janvier 2006 sont prorogées jusqu'au 31 décembre 2012.

Article L34-2 En savoir plus sur cet article...

Modifié par Loi 2004-669 2004-07-09 art. 10 I, III JORF 10 juillet 2004

Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 10 JORF 10 juillet 2004

La prescription est acquise, au profit des opérateurs mentionnés à l'article L. 33-1, pour toutes demandes en restitution du prix de leurs prestations de communications électroniques présentées après un délai d'un an à compter du jour du paiement.

La prescription est acquise, au profit de l'utilisateur, pour les sommes dues en paiement des prestations de communications électroniques d'un opérateur appartenant aux catégories visées au précédent alinéa lorsque celui-ci ne les a pas réclamées dans un délai d'un an courant à compter de la date de leur exigibilité.

Article L34-3 En savoir plus sur cet article...

Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 10 JORF 10 juillet 2004

**30^e Conférence mondiale des commissaires à la protection des données et de la vie privée
Strasbourg, 15-17 octobre 2008**

Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles

Auteur de la proposition : L'Agencia de Protección de Datos (Espagne) et le Préposé fédéral à la protection des données et à la transparence (Suisse)

Coparrains :

- La Commission nationale de l'Informatique et des Libertés (France)
- Le Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Le Garante per la Protezione dei Dati Personali (Italie)
- L'Inspectorat d'Etat à la protection des données de la République de Lituanie
- L'Office pour la protection des données de la République Tchèque
- L'Autorité hellénique de protection des données
- L'Autorité néerlandaise de protection des données
- Le Contrôleur européen à la protection des données
- L'Inspecteur général à la protection des données (Pologne)
- Le Commissaire à la protection des données de l'Irlande
- La Dirección nacional para la protección de los datos de l'Argentine
- L'Agence de protection des données de la Principauté d'Andorre
- L'Office du commissaire à l'information (Royaume Uni)
- La Comissão nacional de la proteção dos dados (Portugal)
- Le Commissaire à la vie privée de Nouvelle Zélande
- Le Data Protection Commissioner of Guernsey
- Le Berliner Beauftragte für Datenschutz und Informationsfreiheit
- L'Agence de protection des données du Pays Basque (Espagne)
- L'Agence de protection des données de la Catalogne (Espagne)
- L'Agence de protection des données de Madrid (Espagne)

La Conférence rappelle que:

- la déclaration adoptée à Venise lors de sa 22^e Conférence ;
- la résolution adoptée à Wroclaw lors de sa 26^e Conférence ;
- la déclaration adoptée à Montreux lors de sa 27^e Conférence ;
- l'initiative de Londres présentée lors de sa 28^e Conférence ;
- la résolution adoptée lors de sa 29^e Conférence ;
- tendent à renforcer le caractère universel du droit à la protection des données et à la vie privée et appellent au développement d'une Convention universelle pour la protection des personnes à l'égard du traitement des données personnelles.
- En particulier dans la déclaration de Montreux, la Conférence appelle l'Organisation des Nations Unies à préparer un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée en tant que droits de l'homme exécutoires. La Conférence appelle également le Conseil de l'Europe, conformément à l'article 23 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère

personnel, à inviter les Etats non membres de cette organisation qui ont une législation de protection des données adéquate, à adhérer à la Convention (STE N° 108) et à son protocole additionnel (STE N° 181).

- Dans la résolution de la 29^e Conférence, les commissaires ont souligné la nécessité de soutenir l'élaboration de normes internationales de protection de la vie privée effectives et universellement acceptées comme un mécanisme pour aider les parties à établir et à démontrer la conformité avec les exigences légales de protection des données et de la vie privée.

La Conférence relève que des efforts encourageants ont depuis lors été entrepris en vue de réaliser ces objectifs et qu'en particulier

- La question d'une Convention universelle est inscrite au programme de travail de la Commission du droit international des Nations Unies ;
- Le Conseil de l'Europe est favorable à l'adhésion d'Etats non membres ayant une législation de protection des données conforme à la Convention STE N° 108 et a décidé de promouvoir l'instrument au niveau mondial ; il a ainsi rappelé la vocation potentiellement universelle de la Convention STE N° 108, notamment lors du Sommet mondial sur la Société de l'information à Tunis en novembre 2005 et dans le cadre des Forums sur la gouvernance de l'Internet à Athènes en 2006 et Rio en 2007 ;
- L'OCDE a adopté le 12 juin 2007 une recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée qui tend notamment à améliorer les cadres nationaux pour l'application des lois sur la vie privée afin que les autorités nationales puissent mieux coopérer avec les autorités étrangères et à élaborer des mécanismes internationaux efficaces destinés à faciliter la coopération transfrontière pour l'application des lois sur la vie privée ;
- Les conférences régionales de l'Unesco en 2005 (Asie-Pacifique) et 2007 (Europe) soulignent le caractère prioritaire de la protection des données ;
- Les initiatives déployées par le groupe de l'article 29 de l'Union européenne pour faciliter la procédure d'adoption de règles d'entreprises contraignantes (BCR) et le développement de solutions contractuelles régissant l'échange transfrontières de données.
- Les chefs d'Etats et de Gouvernements de la francophonie se sont engagés à l'issue de leur XI^e sommet à Budapest en septembre 2006 à intensifier, sur la plan national, les travaux législatifs et réglementaires nécessaires à l'établissement du droit des personnes à la protection des données et à œuvrer, sur le plan mondial, en faveur de l'élaboration d'une convention internationale garantissant l'effectivité du droit à la protection des données ;
- L'APEC a adopté en novembre 2004 des principes directeurs de la vie privée pour renforcer la protection de la vie privée et préserver les flux d'information. En septembre 2007, l'APEC a lancé une initiative « vie privée » pour développer le cadre de mise en œuvre afin d'assurer des flux internationaux de données certifiés qui répondent aux besoins des affaires, diminuent les coûts de conformité, offrent aux consommateurs un recours effectif, permettent aux régulateurs d'agir efficacement et minimisent la charge réglementaire ;
- L'Association francophone des autorités de protection des données (AFAPDP) créée à Montréal en marge de la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée soutient dans ses objectifs l'élaboration d'une convention universelle et les efforts en vue de l'adhésion à la Convention STE N° 108 d'Etats non membres du Conseil de l'Europe ;

- Le réseau ibéro américain de protection des données (RIPD) a adopté une déclaration à l'issue de sa 6^e réunion tenue en Colombie en mai 2008 appelant les conférences internationales à la protection des données et à la vie privée à poursuivre, indépendamment de leur appartenance géographique, leurs efforts en vue de l'adoption d'un instrument juridique commun ;
- Les Autorités de protection des données d'Europe central et oriental (APDCO), lors de leur dernière réunion en juin 2008 en Pologne, ont exprimé leur volonté de poursuivre et de renforcer leurs activités au sein de l'APDCO, en particulier d'élaborer des solutions communes et d'assister les nouveaux membres dans la mise en place de leur législation de protection des données.

La Conférence considère que:

- le droit à la protection des données et à la vie privée est un droit fondamental des personnes indépendamment de leur nationalité et de leur domicile ;
- qu'avec l'expansion de la société de l'information, le droit à la protection des données et à la vie privée est une condition indispensable dans une société démocratique pour garantir le respect des droits des personnes, la libre circulation des informations et une économie de marché ouverte ;
- la globalisation des échanges et des traitements de données personnelles, la complexité des systèmes, les dommages pouvant découler d'une mauvaise utilisation de technologies de plus en plus puissantes et l'augmentation des mesures sécuritaires nécessitent une réponse rapide et adéquate pour garantir le respect des droits et libertés fondamentales et notamment le droit à la vie privée ;
- les disparités persistantes en matière de protection des données et de respect de la vie privée à travers le monde, notamment du fait de l'absence de garantie dans plusieurs Etats, nuit aux échanges de données personnelles et à la mise en place d'une protection des données effective et globale ;
- le développement de règles internationales qui garantissent d'une façon uniforme le respect de la protection des données et de la vie privée est prioritaire ;
- la reconnaissance de ces droits passe par l'adoption d'un instrument juridique universel contraignant consacrant, recensant et complétant les principes communs de protection des données et de respect de la vie privée énoncés dans différents instruments existants et renforçant la coopération internationale entre autorités de protection des données ;
- La mise en oeuvre de lignes directrices développées par des organisations comme l'APEC ou l'OCDE, en particulier celles concernant l'adoption d'un cadre international en vue d'améliorer le respect des droits à la protection des données et à la vie privée lors de flux transfrontières de données est une étape positive pour atteindre cet objectif ;
- L'accession à des instruments contraignants de valeur universelle, tel que la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE N° 108) et son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (STE N° 181), lesquels contiennent des principes de base de la protection des données, est susceptible de faciliter les échanges de données entre Parties ; ces instruments, en effet, prévoient des mécanismes et une plateforme de coopération entre autorités de protection des données, envisagent l'établissement de ces autorités de manière à exercer leurs fonctions en toute indépendance et favorisent la mise en place d'un niveau de protection des données adéquat ;
- la 30^e Conférence internationale de la protection des données est une instance appropriée pour adopter une stratégie visant spécifiquement à la réalisation de ces objectifs.

Par conséquent, la Conférence **renouvelle son appel** d'élaborer un instrument juridique universel contraignant en matière de protection des données et à la vie privée, en **adoptant les résolutions suivantes** :

1. La Conférence soutient les efforts du Conseil de l'Europe pour promouvoir le droit fondamental à la protection des données et à la vie privée. Dès lors, la Conférence invite les Etats membres de cette organisation qui ne l'ont pas encore fait à examiner la ratification de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel ; La Conférence invite les Etats non membres en position de le faire à considérer de donner suite à l'invitation du Conseil de l'Europe d'accéder à la Convention STE N° 108 et à son protocole additionnel. Considérant sa résolution sur l'établissement d'un groupe directeur relatif à la représentation aux réunions d'organisations internationales, la Conférence souhaite également contribuer aux travaux du comité consultatif de la Convention STE N° 108.
2. La Conférence soutient les initiatives de l'APEC, de l'OCDE et d'autres organisations régionales et forums internationaux pour le développement de moyens effectifs de promouvoir de meilleurs standards internationaux de protection des données et de la vie privée.
3. **La Conférence charge un groupe de travail**, coordonné par l'autorité organisatrice de la 31^e Conférence internationale et composé des autorités nationales de protection des données intéressées de rédiger et de soumettre à sa session fermée une **proposition commune d'établissement de normes internationales sur la vie privée et la protection des données personnelles**, selon les critères suivants :
 - de recenser les principes et les droits relatifs à la protection des données à caractère personnel dans les différents environnements géographiques du monde, en faisant en particulier référence aux textes légaux ou autres qui ont rencontrés un large degré de consensus dans les forums régionaux et internationaux;
 - d'élaborer un ensemble de principes et de droits qui, en reflétant et en complétant les textes existants, permet d'atteindre un degré maximum d'acceptation internationale assurant un haut niveau de protection ;
 - évaluer les secteurs dans lesquels ces droits et principes sont applicables, y compris les variantes qui mettent l'accent sur l'harmonisation de leurs champs d'application ;
 - définir, en tenant compte de la diversité des systèmes juridiques, les critères de base qui garantissent leur application effective ;
 - examiner le rôle que doit jouer l'auto-régulation ;
 - formuler des garanties essentielles pour des transferts internationaux de données meilleurs et plus souples.

Le processus de rédaction de cette proposition conjointe doit être effectué en encourageant une large participation aux groupes de travail et à des forums ou des auditions, des organisations et entités publiques ou privées, en vue d'obtenir le plus large consensus institutionnel et social. Une attention particulière devrait être accordée aux travaux en cours de l'Organisation internationale de normalisation (ISO) et de la Commission du droit international.

Levallois, le 10 février 2009

COMMUNIQUÉ DE PRESSE

La fréquentation des sites Internet français Classement CybereStat des sites souscripteurs de l'étude Médiamétrie-eStat

Janvier 2009

Près de 4 fois plus de visites issues de mobiles en un an

Source : Classement CybereStat - Copyright Médiamétrie-eStat - Tous droits réservés

Médiamétrie-eStat publie ce mois-ci un **bilan sur les visites issues de mobiles** et en particulier de l'**iPhone** et de l'**iPodTouch** ainsi que les résultats du classement CybereStat de **32 groupes et 71 sites**. **Groupe ConcoursMania**, **Groupe vocation service public** et **YouJob.com** viennent enrichir la publication de Médiamétrie-eStat pour le mois de janvier 2009.

Plus d'une visite mobile sur 2 provient d'un iPhone ou d'un iPodTouch

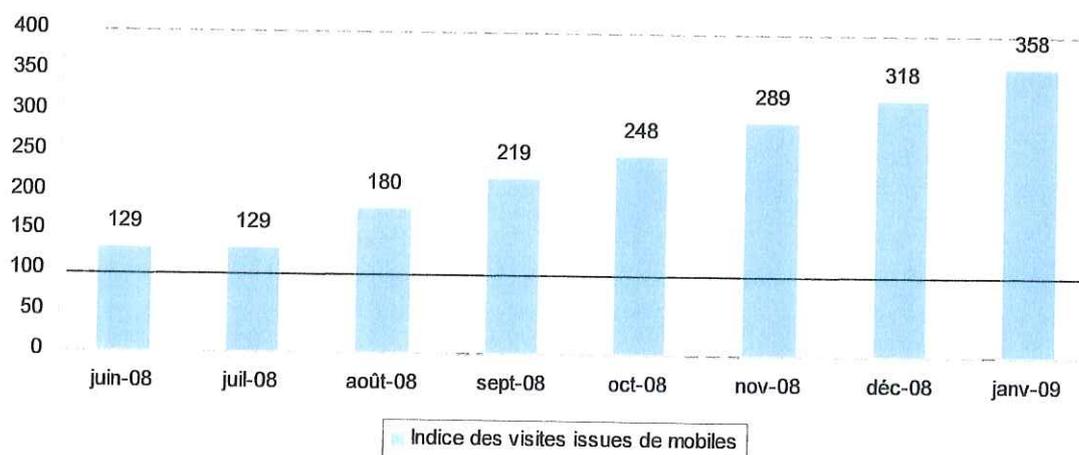
Entre janvier 2008 et janvier 2009, les **visites** en provenance de **mobiles** ont presque été **multipliées par 4**. Elles représentent cependant 0,45% du total des visites sur les sites mesurés par Médiamétrie-eStat.

Cette croissance a été en grande partie boostée par l'**iPodTouch** et l'**iPhone** puisque ces accès représentent **68% de la progression** globale des visites issues de mobiles.

Les **2 plus fortes progressions** (en valeur) en provenance de l'**iPhone** ont eu lieu entre juillet et août (**+73% de visites**) et pendant les **fêtes de fin d'année** c'est-à-dire entre décembre et janvier (**+19% de visites**).

Au total en janvier 2009, l'**iPhone** et l'**iPodTouch** représentent **55% des provenances mobiles** en termes de visites sur le périmètre des sites mesurés.

Evolution de l'indice des visites issues de mobiles
(la base 100 est le total des visites issues de mobiles en janvier 2008)



Le Classement CybereStat des GROUPES - Janvier 2009

	GROUPES	Total des visites ⁽²⁾		Durée moyenne de la visite ⁽⁴⁾
		MOIS NORME ⁽³⁾ JANVIER 2009	EVOLUTION VS. MOIS NORME ⁽³⁾ DECEMBRE 2008	JANVIER 2009
1	Groupe Skyrock	210 506 304	+1%	00:22:55
2	Groupe Pages Jaunes	77 675 428	+15%	00:05:37
3	Groupe Lagardère Active	66 956 340	+7%	00:15:01
4	Groupe L'Equipe	59 988 488	+18%	00:21:05
5	Groupe EoRezo	55 105 360	+7%	00:14:09
6	Groupe Dreamnax - Sexyavenue	52 374 133	+19%	00:10:06
7	Groupe Rentabiliweb	39 481 599	+10%	00:09:15
8	Groupe France Télévisions	36 212 455	+14%	00:13:33
9	Groupe Internext	35 894 862	0%	00:07:08
10	Groupe Le Figaro	34 507 984	+14%	00:16:13
11	Groupe AdThink Media	15 484 309	+1%	00:09:10
12	Groupe United Champions France	14 284 550	+20%	00:06:01
13	Groupe M6	14 093 536	+5%	00:08:31
14	Groupe Index Multimédia	13 712 946	+1%	00:48:01
15	Groupe Seloger.com	12 755 105	+37%	00:12:51
16	Groupe Radiofrance	8 827 624	+17%	00:06:31
17	Groupe Mediastay France	8 779 310	-	00:09:20
18	Groupe PAP	7 436 394	+46%	00:09:30
19	Groupe Mondadori France Digital	4 903 690	+22%	00:04:06
20	Réseau Métaboli	3 304 538	+11%	00:05:24
21	Groupe Studyrama	3 212 865	+49%	00:08:38
22	Groupe Moniteur	2 804 867	+14%	00:06:47
23	Groupe Skiadvertising	2 501 023	+9%	00:09:45
24	Groupe UpToTen	2 243 413	-8%	00:44:12
25	Groupe Turf Editions	2 101 205	+7%	00:09:43
26	Groupe Musicme	1 775 619	+44%	00:11:15
27	Groupe ConcoursMania	1 187 353	-	00:07:50
28	Groupe Universal Music	569 798	-14%	00:06:33
29	Groupe Les Inrockuptibles	513 102	+10%	00:21:33
30	Groupe vocation service public	503 297	-	00:09:47
31	Groupe Le Site Immo	363 049	+43%	00:06:45
32	Groupe Runweb	94 069	+9%	00:06:28

Le Classement CybereStat des SITES – Janvier 2009

	SITES (Groupe)	Total des visites ⁽²⁾		Durée moyenne de la visite ⁽⁴⁾
		MOIS NORME ⁽³⁾ JANVIER 2009	EVOLUTION VS. MOIS NORME ⁽³⁾ DECEMBRE 2008	JANVIER 2009
1	Skyrock.com (Groupe Skyrock)	209 629 440	+1%	00:22:57
2	L'Equipe.fr (Groupe L'Equipe)	56 358 350	+18%	00:21:13
3	Over-blog	53 903 000	+5%	00:11:31
4	LO.ST (Groupe EoRezo)	49 641 268	+5%	00:14:45
5	Doctissimo.fr (Groupe Lagardère Active)	34 700 040	+13%	00:12:40
6	Alice	31 154 504	+5%	00:15:16
7	01net (Groupe Internext)	31 005 425	-1%	00:07:06
8	France 2 (Groupe France Télévisions)	16 231 967	+21%	00:10:18
9	France 3 (Groupe France Télévisions)	15 320 759	+2%	00:17:23
10	pmu.fr	9 355 100	+8%	00:13:00
11	Tchatte.com (Groupe Index Multimédia)	8 323 565	+1%	00:53:32
12	pap.fr (Groupe PAP)	6 704 764	+45%	00:09:09
13	Francefootball (Groupe L'Equipe)	5 665 458	+14%	00:13:50
14	TV5 Monde	5 041 715	+18%	00:08:43
15	Ados.fr (Groupe Lagardère Active)	4 760 703	-8%	00:08:18
16	France 5 (Groupe France Télévisions)	4 751 994	+22%	00:09:20
17	Homelidays	4 392 340	+77%	00:12:59
18	Kingoloto FR (Groupe Mediastay France)	4 118 102	-	00:06:19
19	RMC.fr (Groupe Internext)	4 099 466	+1%	00:07:07
20	Fluctuat.net (Groupe Lagardère Active)	3 932 151	+7%	00:05:53
21	babel.com (Groupe Index Multimédia)	3 767 714	+3%	00:50:45
22	01men (Groupe Internext)	3 377 984	0%	00:06:29
23	Europe 1 (Groupe Lagardère Active)	2 912 021	+21%	00:20:05
24	Site des marques	2 772 117	+15%	00:04:19
25	La Tribune	2 762 694	-3%	00:17:50
26	Kingomusic FR (Groupe Mediastay France)	2 709 441	-	00:07:48
27	E-santé	2 693 592	+37%	00:06:32
28	Mediatico	2 547 527	+22%	00:06:47
29	Bananalotto FR (Groupe Mediastay France)	2 216 650	-	00:05:33
30	Aina Media	1 869 671	-6%	00:12:33
31	Citegay	1 858 383	+3%	00:20:08
32	Grattage FR (Groupe Mediastay France)	1 668 957	-	00:10:22
33	purevoyance.com	1 534 628	+12%	00:06:36
34	Psychologies.com	1 429 623	+5%	00:13:11
35	Skipass.com (Groupe Skiadvertising)	1 412 987	+5%	00:08:50
36	Virgin Radio (Groupe Lagardère Active)	1 370 183	-9%	01:28:13
37	MCM (Groupe Lagardère Active)	1 340 167	-12%	00:07:19
38	Booska-p	1 304 094	-13%	00:11:25
39	Entreparticuliers.com	1 303 733	+29%	00:06:18
40	Momes.net (Groupe Lagardère Active)	1 210 651	-16%	00:06:04
41	Paris Turf (Groupe Turf Editions)	1 160 003	+11%	00:09:26
42	Tiercé magazine (Groupe Turf Editions)	1 070 065	+2%	00:08:38
43	BFM (Groupe Internext)	1 040 305	+44%	00:05:51
44	Masculin.com	1 001 028	+28%	00:06:45
45	YouJob.com*	977 965	-	00:08:21
46	France 4 (Groupe France Télévisions)	931 887	+140%	00:09:47
47	Francetvod (Groupe France Télévisions)	859 863	+5%	00:04:31
48	Myblog.fr (Groupe Lagardère Active)	764 824	-1%	00:06:32
49	Gulli (Groupe Lagardère Active)	720 142	-24%	00:10:21
50	Cité des Sciences	652 440	+18%	00:07:52
51	RFO (Groupe France Télévisions)	626 955	+22%	00:08:11
52	Site-pap.fr (Groupe PAP)	514 063	+61%	00:06:33
53	equidia.fr	471 546	+4%	00:03:21
54	Les Inrockuptibles (Groupe Les Inrockuptibles)	460 032	+11%	00:21:41
55	lemondeinformatique.fr (Groupe AdThink Media)	333 773	+10%	00:05:50
56	Villanao.fr	320 976	+114%	00:08:47

	SITES (Groupe)	Total des visites ⁽²⁾		Durée moyenne de la visite ⁽⁴⁾
		MOIS NORME ⁽³⁾ JANVIER 2009	EVOLUTION VS. MOIS NORME ⁽³⁾ DECEMBRE 2008	JANVIER 2009
57	Canal J (Groupe Lagardère Active)	300 805	-3%	00:10:50
58	Talents.fr	294 030	+14%	00:03:59
59	Gyneweb.fr (Groupe Lagardère Active)	289 678	+20%	00:06:21
60	Opéra de Paris	287 721	-34%	00:06:42
61	Mad Movies	241 099	+5%	00:12:07
62	Toutpartout.com (Groupe Lagardère Active)	197 130	+9%	00:05:37
63	unhomme.fr (Groupe AdThink Media)	190 243	-9%	00:05:41
64	Mood.fr	163 131	-1%	00:10:47
65	Gnomz.com (Groupe Lagardère Active)	101 569	0%	00:09:11
66	reseaux-telecoms.net (Groupe AdThink Media)	93 812	+44%	00:05:34
67	digitalworld.fr (Groupe AdThink Media)	71 675	+23%	00:04:54
68	DoubleTrade	65 279	+17%	00:13:32
69	distributive.com (Groupe AdThink Media)	57 522	+31%	00:06:13
70	cio-online.com (Groupe AdThink Media)	17 453	+23%	00:06:32
71	Mesdiscussions.net (Groupe Lagardère Active)	13 183	+11%	00:03:18

* Pour des raisons indépendantes de Médiamétrie-eStat, la mesure du site Youjob.com a démarré le 12 janvier.

► Liste des principaux domaines associés aux groupes et sites publiés. Cette précision permet d'avoir une vue globale de l'ensemble des sites mesurés.

Remarque : la mention étoile (*) signifie que le site comporte des sous-domaines qui appartiennent aux URLS déclarées par le site. Par exemple, une URL se lit de la façon suivante : sousdomaine.domaine.fr.

Groupes :

Groupe AdThink Media ⁽⁵⁾ : adthink-media.com ; advertstream.com ; adsmarketplace.com ; cio-online.fr ; digitalwold.fr ; distributive.fr ; lemondainformatique.fr ; ludokado.com ;

rencontres-faciles.fr ; renkontre.com ; reseaux-telecoms.net ; unhomme.fr "

Groupe ConcoursMania : concours.fr ; revuedesjeux.com ; kado.fr ; conso.fr ; adconcours.com

Groupe DreamNex – Sexyavenue ⁽⁶⁾ : sexyavenue.com ; sexyavenue.it ; sexyavenue.co.uk ; dreamnex.com ; protegezvosenfants.org

Groupe EoRezo : eorezo.com ; *.lo.st ; *.eo.st ; *.in.st ; ulimit.com ; *.be.tf ; *.best.cd ; *.bsd-fan.com ; *.c0m.st ; *.ca.tc ; *.clan.st ; *.com02.com ; *.en.st ; *.euro.st ; *.fr.fm ; *.fr.st ; *.fr.vu ; *.gr.st ; *.ht.st ; *.int.ms ; *.it.st ; *.java-fan.com ; *.linux-fan.com ; *.macfan.com ; *.mp3.ms ; *.qc.tc ; *.sp.st ; *.suisse.st ; *.t2u.com ; *.unixlover.com ; *.zik.mu

Groupe France Télévisions : france2.fr ; france3.fr ; france4.tv ; france5.fr ; francetv.fr ; francetvod.fr ; casediscute.com ; emission-union-libre.com ; x-bourse-france2.axime.com ; rfo.fr

Groupe Index Multimédia : amitie.fr ; amour.fr ; babel.com ; badmobile.com ; cybermen.com ; drague.net ; everykindofpeople.com ; gay2424.com ; hitmobile.com ; indexmultimedia.com ; indexmultimedia.fr ; logosonnerie.com ; magikmobile.com ; magiksms.com ; meexup.com ; planlibertin.com ; recremobile.com ; recremobile.fr ; sonnerieslogos.com ; tchatte.com ; tchatte.tv ; tchatteblog.com ; 123sat.com ; habitbi.com

Groupe Internext : 01men.com ; 01net.com ; bfmv.fr ; microachat.com ; radiobfm.com ; rmc.fr

Groupe Lagardère Active : ados.fr ; beauty-experts.com ; canalj.net ; deki0.fr ; doctissimo.fr ; elle.fr ; europe1.fr ; europe2.fr ; europe2.horoscope.fr ; europe2rock.fr ; europe2tv.fr ; femina.fr ; fillestv.com ; fluctuat.net ; gnomz.com ; gulli.fr ; gyneweb.fr ; infobebes.com ; lejdd.fr ; mcm.net ; mcm.vl-wl.com ; mcmbe.tv ; mesdiscussions.net ; memes.net ; mood.fr ; myblog.fr ; parents.fr ; parismatch.com ; pixelmonde.fr ; premiere.fr ; psychologies.com ; psychologies.fr ; public.fr ; quelpsy.psychologies.com ; questionsexo.psychologies.com ; rfm.fr ; tele7.fr ; tiji.fr ; test-et-vous.psychologies.com ; toutpartout.com ; virgin17.fr ; virginradio.fr ; virginradio.vl-wl.com ; virginradioblog.fr ; visez.com

Groupe Le Figaro : figaro.net ; figaroeconomie.com ; figaroeconomie.fr ; figaroetudiant.com ; figaro-etudiant.com ; figaroetudiant.fr ; figaromadame.com ; figaromadame.fr ; figaroscope.biz ; figaromagazine.fr ; figaromagazine.com ; figaroscope.com ; figaroscope.fr ; figaroscope.info ; figaroscope.net ; figaroscope.org ; franceamerique.figaro.net ; groupe-figaro.fr ; explorimmo.com/cobranding/FIGARO ; jdf.com ; jdf.fr ; jfinances.com ; jobscampus.com/partenaire/figaro ; journaldesfinances.com ; journaldesfinances.fr ; lasolitaire.com ; lefigaro.com ; le-figaro.com ; lefigaro.fr ; lefigaroeconomie.fr ; lefigaroetudiant.com ; lefigaro-etudiant.com ; lefigaroetudiant.fr ; lefigaroscope.com ; lefigaroscope.fr ; lefigaroscope.net ; lyon-figaro.com ; madame.lefigaro.fr ; madamefigaro.com ; madamefigaro.fr ; sport24.com ; sport24.fr ; tvmag.com ; tvmag.fr ; tvmagazine.com ; tvmagazine.fr ; cadremploi.fr/emploi/recherche_offres?cob=_figaro ; mareussite.com/lefigbilan ; evene.fr ; ticketac.com

Groupe Le Site Immo : www.lesiteimmo.com ; www.le-site-immo.com ; www.iledefrance-immobilier.com ; www.beaujolais-immobilier.com ; www.immobilier-champagne.com ; www.immobilier-bourgogne.com ; www.immobilier-alsace.com ; www.drome-immobilier.com ; www.doubs-immobilier.com ; www.jura-immobilier.com ; www.auvergne-immobilier.com ; www.macon-immobilier.com ; www.immobilier-rhone.com ; www.immobilier-grenoble.net ; www.immobilier-lyon.net ; www.immobilier-annecy-74.com ; www.immobilier-rennes-35.com ; www.immobilier-avignon-84.com ; www.immobilier-toulouse-31.com

Groupe L'Equipe : lequipe.fr ; equipe.fr ; lequipe.com ; lequipeauto.fr ; lequipe.tv ; equipe.tv ; francefootball.fr ; velomagazine.fr

Groupe Les Inrockuptibles : www.lesinrocks.com ; www.cqfd.com

Groupe M6 : *.m6.fr ; m6boutique.com ; girondins.com ; turbo.fr ; turboblog.fr

Groupe Mediastay France : bananalotto.fr ; grattage.fr ; kingoloto.fr ; kingomusic.fr

Groupe Mondadori France Digital : 20ans.com ; addxonline.fr ; autojournal.fr ; autoplus.fr ; bateauxonline.fr ; bibamagazine.fr ; canalstars.fr ; closermag.com ; clubchats.com ; courseonline.fr ; fhm.fr ; francecamping.com ; francegolf.fr ; guidetele.com ; kiosquemap.com ; lechasseurfrancais.com ; max-magazine.com ; modesetravaux.com ; pleinevie.fr ; studiomagazine.com ; topsante.fr ; telepoche.fr ; telestars.fr

Groupe Moniteur : *batiprix.com ; *batiproduits.com ; *courrierdesmaires.com ; *courrierdesmaires.fr ; *editionsdumoniteur.com ; *emploipublic.fr ; *enerpresse.com ; *entrepreneur-expert.com ; *equipment-center.com ; *batitextes.com ; *groupemoniteur.fr ; *lagazettedescommunes.com ; *lagazette.fr ; *lagazette-sante-social.com ; *gazette-sante-social.fr ; *lemoniteur-emploi.com ; *lemoniteur-expert.com ; *librairiedumoniteur.com ; *marchesonline.com ; *operationsimmobilières.com ; *mapaonline.fr ; *batiproduits-maison.com ; *lemoniteur.fr ; *ame1901.fr ; *carrieres-publiques.com ; *infosport.org ; *metier-securite.fr ; *modeles-experts.com ; *technicites.fr ; *territorial.fr ; *territorial-recrutement.fr ; *tessolidaire.com

Groupe Musicme : www.musicme.com ; musique.01net.com ; hostile.fm ; en.musicme.com

Groupe Pages Jaunes : www.pagesjaunes.fr ; www.quidonc.fr

Groupe PAP : pap.fr ; papvacances.fr ; site-pap.fr ; demeures-de-charme.com ; construisesamaison.com ; immoneuf.com ; bureaux-commerces.com ; journaldesparticuliers.com ; bcti.fr

Groupe Radio France : *.radiofrance.fr ; *.franceinfo.fr ; players.tv-radio.com/radiofrance

Groupe Rentabiliweb ⁽⁵⁾ : www.palmars.com ; www.toox.com ; www.groomradio.com ; www.rentabiliweb.com ; www.yes-messenger.com ; www.mailorama.fr ; www.eurolive.com ; www.128b.com ; www.0instant.com ; www.takepass.com ; www.protectiondesmineurs.com ; www.coinchegratuit.com ; www.yams-gratuit.com ; www.dames-gratuit.com ; www.belote-gratuit.com ; www.mykodial.com ; www.purfirt.com

Groupe RunWeb : http://www.runweb.com, http://reunion.runweb.com, http://maurice.runweb.com, http://beijing.runweb.com, http://forums.runweb.com, http://www.arhes.com, http://www.arhes-immobilier.com, http://www.varanga.com

Groupe SeLoger.com : *immostreet.com ; *immostreet.fr/ ; immostreet.aliceadsl.fr ; immobilier.club-internet.fr/ ; *seloger.com ; *seloger.net ; seloger.money.msn.fr ; seloger.immobilier.orange.fr ; seloger.orange.fr ; immobilier.neuf.fr ; immobilier.cegetel.net ; immo.capital.fr ; selogerpro.com ; pressimmo-online.com ; pressimmo.fr ; selogerneuf.com ; groupe-seloger.com ; groupeseloger.com"

Groupe Ski-Advertising : www.skihorizon.com ; www.skipass.com ; www.totem-voyages.com ; www.skihoo.com ; www.zapiks.com

Groupe Skyrock : skyrock.com ; skyrock.fm ; tasante.com ; tropmalin.com ; bonbiz.net ; ladiz.fr ; skyrockmobile.com ; skyrockmessenger.com

Groupe Studyrara : Studyrara –budget ; Hobsons.fr ; focusRH ; focusCO ; observatoiredesalaires.fr ; vivreaetranger.fr ; Studyrara-fp ; groupe-studyrara.com ; jeunes-mag.com ; mapiaule.com ; studyrara.com ; studyrara-emploi.com ; studyrara-jobs.com ; studyrara-pro.com ; studyrara-direct.com

Groupe Turf Editions : tierce-magazine.fr ; tierce-magazine.com ; paris-turf.com

Groupe United Champions France : footmercato.net ; clickshoot.fr ; click-shoot.sports.orange.fr ; click-shoot.aol.fr

Groupe Universal Music : universalmusic.fr ; e-compil.fr ; arthurh.net ; bernardlavilliers.com.fr ; calogero.com.fr ; daniellevy.net ; daniel-mille.com ; davidhalliday.net ; depalmas.net ; eddymitchell.net ; florentpagny.net ; georgesbrassens.com.fr ; jeanguillou.org ; johnnyhallyday.com ; l5.fr ; maximeleforestier.com.fr ; michelsardou.net ; prophet-worldmusic.com ; rickallison.com ; sergegainsbourg.com.fr ; souadmassi.com.fr ; zazieonline.com

Groupe UpToTen : uptoten.com ; boowakwala.jeunesse.orange.fr

Groupe vocation service public : concours.mobilite-territoriale.net ; vocationfonctionnaire.fr

Réseau Métaboli ⁽⁵⁾ : jeuxvideo.wanadoo.fr ; www.metaboli.fr ; metaboli.clubic.com ; gamekult.metaboli.fr ; metaboli.club-internet.fr ; gameone.metaboli.fr ; aol.metaboli.fr ; www.neufgame.fr ; www.metaboli.co.uk ; fnac.metaboli.fr ; packardbell.metaboli.fr ; fnac.gamesplanet.com ; www.metaboli.de ; www.gamesplanet.com ; metaboli.numericable.fr ; fun.metaboli.fr ; allocine.metaboli.fr ; packardbell.metaboli.co.uk ; metaboli.tele2internet.fr ; metaboli.noos.fr ; metaboli.goa.com ; numericable.metaboli.fr ; metaboli.wanadoo.fr ; cvg.metaboli.co.uk ; metaboli.rtl.fr ; ncn.metaboli.fr ; gamesonradar.metaboli.co.uk ; funsta.metaboli.co.uk ; rtl.metaboli.fr ; surcouf.metaboli.fr ; metaboli.funradio.fr ; noos.metaboli.fr ; www.metaboli.fr ; wanadoo.metaboli.fr ; http://pixmania.metaboli.fr ; http://www.metaboli.it

Sites :

01men : 01men.com

01net : 01net.com

Ados.fr : ados.fr

Aina Media : rap2k.com

Alice : *aliceadsl.fr ; aliceadsl.fou.fr ; aliceadsl.lci.fr ; aliceadsl.eurosport.fr ; aliceadsl.plurielles.fr ; emissionstf1.aliceadsl.fr

babel.com : www.babel.com

Bananalotto FR : bananalotto.fr

BFM : bfm.fr ; radiobfm.com

Booska-p : booska-p.com

Canal J : canalj.net

Cio-online.com : cio-online.com

Cité des Sciences : cite-sciences.fr

Citégay : citegay.com

digitalworld.fr : digitalworld.fr

Distributique.com : distributique.com

Doctissimo.fr : doctissimo.fr

DoubleTrade : doubletrade.com/fr

Entrepaticuliers.com : entreparticuliers.com ; entreparticuliers.fr

equidia.fr : equidia.fr

E-santé : e-sante.fr

Europe 1 : europe1.fr
Fluctuat.net : fluctuat.net
France 2 : france2.fr
France 3 : france3.fr
France 4 : france4.fr
France 5 : france5.fr
Francefootball : francefootball.fr
Francetvod : francetvod.fr
Gnomz.com : gnomz.com
Grattage FR : grattage.fr
Gulli : gulli.fr
Gyneweb.fr : gyneweb.fr
Homelidays : homelidays.com
Kingoloto FR : kingoloto.fr
Kingomusic FR : kingomusic.fr
La Tribune : latribune.fr, latribune.com, latribune.ar.wilink.com, efinancialcareers.com, latribune.efinancialcareers.fr, latribune.sports.fr, lamp.latribune.migration.lbn.fr
Lemondeinformatique.fr : lemondeinformatique.fr
L'Equipe.fr : lequipe.fr; equipe.fr; lequipe.com; lequipeauto.fr; lequipetv.fr; equipetv.com
Les Inrockuptibles : lesinrocks.com
LO.ST : *.lo.st
Mad Movies : mad-movies.com
Masculin.com : masculin.com
MCM : mcm.net
Mediadico : mediadico.com
Mesdiscussions.net : mesdiscussions.net
Momes.net : momes.net
Mood.fr : mood.fr
Myblog.fr : myblog.fr
Observatoire de la franchise : observatoirede lafranchise.fr
Opéra de Paris : opera-de-paris.fr ; operadeparis.fr ; resa.opera-de-paris.fr
Over-blog : *.over-blog.com ; *.over-blog.net ; *.over-blog.org
pap.fr : pap.fr
Paris Turf : paris-turf.com
pmu.fr : pmu.fr
Psychologies.com : psychologies.com ; psychologies.fr ; quelpsy.psychologies.com ; questionsexo.psychologies.com ; test-et-vous.psychologies.com ; purevoyance.com
Reseaux-telecoms.net : reseaux-telecoms.net
RFO : rfo.fr
RMC.fr : rmc.fr
Site des marques : sitedesmarques.com
Site-pap.fr : site-pap.fr
Skipass.com : skipass.com
Skyrock.com : skyrock.com
Talents.fr : bale.fr ; emploi.multimedia.telerama.fr ; talents.fr ; talents.site-recrutement.com ; talents.keljob.com
Tchatte.com : tchatte.com
Tiercé Magazine : tierce-magazine.fr ; tierce-magazine.com
Toutpartout.com : toutpartout.com
TV5 Monde : tv5.org, tv5.fr, tv5.ca ; tv5.de; tv5info.com ; tv5info.nl ; tv5info.org ; tv5monde.com ; tv5monde.jp ; tv5monde.org ; tv5musique.org ; tv5.allocine.fr ; tv5.vodeo.tv; cartes.tv ; cites.tv ; francoffonies.fr ; funnycards.tv ; xe.com/ucc/tv5; http://a455.g.akamai.net
unhomme.fr : unhomme.fr
Villanao.fr : villanao.fr
Virgin Radio : virgin17.fr ; virginradio.fr ; virginradio.vm-wl.com ; virginradioblog.fr
YouJob.com : youjob.com

(⁵) : Principales urls - liste non exhaustive

► Définitions

- (1) **L'indice des visites et de la durée moyenne** est calculé sur la base d'un périmètre de sites constants à partir de janvier 2009. Si après janvier 2009, un site sort de ce périmètre, ses résultats sont estimés jusqu'en décembre 2009. A chaque premier janvier, le périmètre des sites est redéfini.
- (2) **Visite de site** : consultation d'un site, c'est-à-dire chargement par l'internaute d'au moins une page d'un site web. Plusieurs visites peuvent correspondre au même visiteur.
- (3) **Mois normé** : mois théorique composé d'un nombre de jours et de week-ends fixe (30,4375 jours, soit 2/7^{ème} de jours de week-ends pour 5/7^{ème} de jours de semaine). Utilisé pour la comparaison des visites mois par mois, il compense les variations du nombre de jours et de week-ends des mois existants.
- (4) **Durée moyenne de la visite** : il s'agit de la somme totale des durées de visite enregistrées divisée par le nombre total de visites enregistrées dans le mois pour le site. La durée moyenne de la visite est exprimée en minutes et secondes (hh:mm:ss)

► **A propos de Médiamétrie-eStat**

Médiamétrie-eStat est l'opérateur de référence en France de la mesure du trafic Internet «site centric», fondée sur une technologie de marqueur installé directement sur le site Internet. Les solutions commercialisées par Médiamétrie-eStat couvrent les besoins des sites en matière de pilotage des stratégies sur l'Internet fixe et mobile.

Cette mesure propose le suivi très précis du comportement de l'internaute. Elle identifie les contenus les plus consultés, l'origine des visites, l'efficacité des actions de marketing en ligne...eStat mesure également le streaming, le podcast et l'Internet mobile et propose une mesure "live" des flux streamés avec Radio Live et Video Live.

Avec sa nouvelle interface d'accès aux résultats, Médiamétrie-eStat s'inscrit dans l'ère 2.0. Sa technologie a été pensée pour anticiper les changements à venir, et rendre opérationnel le rapprochement avec la mesure du panel Médiamétrie//NetRatings.

Chaque client de Médiamétrie eStat – plus de 850 au total - dispose d'une interface dédiée. Les résultats sont disponibles en temps réel et à J+1.

Les clients qui souhaitent publier leurs résultats sont intégrés au présent classement mensuel CybereStat.

Pour plus d'informations sur les solutions de Médiamétrie-eStat, visitez le site : www.mediametrie-estat.com

Pour toute information presse contacter :

Laure Osmanian Molinero

Tél. : 01 47 58 97 55 - Fax : 01 47 58 09 26

E-mail : losmanian@mediametrie.fr

Annexe 8**Inactivité des comptes**

- Au delà d'un an d'inactivité de votre compte Yahoo!, celui-ci (c'est-à-dire votre identifiant) peut être supprimé à tout moment, sans information préalable. Vous perdrez donc votre identifiant, qui pourra être réattribué le cas échéant à un autre internaute. Passé ce délai d'un an d'inactivité, vous ne pourrez plus accéder (i) ni aux services Yahoo! nécessitant l'ouverture d'une session, (ii) ni aux différents contenus/informations que vous auriez pu stocker sur ces services. Vous ne pourrez pas récupérer votre identifiant.
- Cette règle est applicable au compte Yahoo!, des règles spécifiques, notamment concernant les services Yahoo! Mail, Flickr, Porte-Document et Yahoo! Groupes, peuvent entraîner une suppression plus rapide de vos contenus sur ces services. Veuillez vous reporter aux pages du Centre Yahoo! Données Personnelles spécifiques à ces services. [Cliquez ici](#) pour accéder à la liste complète des produits.

Partage et divulgation des données

En aucun cas, Yahoo! ne partagera ni ne divulguera vos données personnelles en dehors du Groupe Yahoo!, excepté dans les cas suivants. Yahoo! ne transmet vos données personnelles à un tiers que :

- lorsque vous nous avez donné votre accord préalable pour le partage de ces informations (p.ex. pour des opérations de marketing direct) ;
- lorsque nous devons partager ces informations avec les fournisseurs, prestataires et notamment nos prestataires techniques, vendeurs, acheteurs, pour vous permettre d'utiliser le produit ou vous fournir le service que vous avez demandé (p.ex. lorsque vous faites une réservations sur Yahoo! Voyages) ;
- lorsque, pour des raisons de gestion, de conservation et de sécurité des informations recueillies, vos données sont transférées aux États-Unis et stockées sur des serveurs appartenant à Yahoo! Inc. ;
- lorsque nous recevons la requête d'une autorité judiciaire ou de toute autorité administrative habilitée par la loi sollicitant la communication de ces informations conformément aux dispositions législatives.

Pour plus d'informations, vous pouvez consulter notre rubrique relative au [Partage de données](#)

Cookies

- Yahoo! se réserve le droit, aux bonnes fins d'utilisation de ses services, de placer des « cookies » sur votre ordinateur et d'y accéder. En particulier, Yahoo! utilise les cookies pour assurer la gestion des sessions que vous ouvrez sur les services personnalisés avec votre compte Yahoo! et/ou pour personnaliser l'affichage des bandeaux publicitaires sur les sites du Groupe Yahoo! ou sur les sites partenaires de Yahoo!.
- Veuillez noter que lorsque vous accédez, en cliquant sur leurs bandeaux, aux sites faisant de la publicité sur Yahoo! ou simplement en visualisant, au cours de votre visite sur notre site, de tels bandeaux publicitaires, des cookies peuvent être placés sur votre disque dur par les sociétés diffusant ces publicités. Yahoo! n'a aucun accès à ces cookies ou autres fonctionnalités que ces sociétés peuvent être amenées à utiliser. L'utilisation de tels cookies relève de la politique de gestion des données personnelles de ces sociétés que nous vous conseillons de consulter.
- Vous trouverez de plus amples détails sur les cookies dans cette [page sur les cookies](#). Dans cette page, nous vous rappelons aussi les moyens vous permettant de paramétrer votre navigateur pour neutraliser ou refuser le placement des cookies. Notez que, en empêchant le placement de cookies sur votre ordinateur, les services Yahoo! accessibles via un compte vous seront alors inaccessibles.

Balises Web

- Yahoo! utilise des [balises web](#) pour accéder aux cookies exploités sur son propre réseau de sites web par les différents produits et services Yahoo!

Conservation des données

- Vos données nominatives sont conservées le temps de l'utilisation de votre compte, augmenté d'un délai de 90 jours à compter de la demande de suppression de votre compte, pour réserver votre ancien nom de compte et éviter que certains utilisateurs ne le ré-exploitent dans une intention maligne

La sortie de Chrome, le navigateur de Google, a mis en lumière les visées du géant sur nos données personnelles.

Au point qu'il a même inquiété la Cnil.



GOOGLE en sait-il trop sur vous ?

Comme c'est curieux...

- **PAS D'IDENTIFICATION DANS STREET VIEW.** Les Cnil européennes ont veillé à ce que les clichés pris dans le cadre du service Google Street View (photos panoramiques de rues) respectent la vie privée des européens. Aussi, les plaques d'immatriculation des véhicules ainsi que les visages sont-ils floutés a priori – ils ne le sont qu'a posteriori aux États-Unis, sur demande expresse. Mais pour la Cnil, "le système n'est pas fiable à 100 %"...
- **NOS COURRIERS LUS ET ANALYSÉS DANS GMAIL.** Pour placer de la publicité en rapport avec nos courriers Gmail, Google les lit tous et les analyse. De plus, le service s'autorise à conserver les messages même si l'utilisateur les a effacés ou a fermé son compte. Dès 2004, la Cnil se montrait préoccupée par cet aspect du service. Réponse de Google : ce ne sont que des machines qui nous lisent, pas des humains...
- **LA CONSERVATION DES DONNÉES.** En octobre 2007, la Cnil s'inquiétait, devant le Sénat, de la durée de conservation des données par Google, et de sa capacité à agréger des données éparses pour établir un profil détaillé de millions de personnes. En avril 2008, les Cnil européennes recommandaient une conservation de six mois au lieu des dix-huit pratiqués par le moteur. En septembre dernier, Google passait à neuf mois de conservation, mais toujours sans vouloir reconnaître les lois européennes, alors qu'il a des serveurs et des établissements en Europe.

Chrome, le navigateur de Google, a bien des qualités : léger, sobre, très rapide sur les sites modernes faisant grand usage du Javascript, sécurisé dans son architecture avec un processus mémoire différent pour chaque onglet, navigation privée intégrée, etc. Et pourtant, sa sortie aura souligné, plus que jamais, les risques qui pèsent sur notre vie privée face à la moissonneuse de données privées qu'est le géant de la recherche sur Internet.

Ce n'est pas la première fois que Google et les traces qu'il collecte nous concernant nous jouent des tours... et jusque dans notre vie familiale ! Voilà la mésaventure qu'a connue M. Robert, et qui pourrait arriver à chacun de

PHOTO JACQUES FEINE

[Vers le portail Alizé](#)**Annexe 9bis**

Centre de ressources documentaires

[Accueil](#) | [Fiscalité](#) | [Droit](#) | [Questions sociales](#)[Informatique](#) | [Gestion publique](#) | [Economie](#)[Accueil](#) > [Informatique](#) > [Dossiers](#) > [Les 10 ans d'un leader \(I\) : Google et la vie privée des internautes](#) >

Les 10 ans d'un leader (I) : Google et la vie privée des internautes

En 10 ans, Google est devenu un acteur majeur d'internet. Le moteur de recherche fondé en 1998 par Larry Page et Sergey Brin est désormais une marque mondialement connue et un acteur majeur des réseaux dont les activités s'étendent bien au-delà de la recherche d'information. Gestion de courrier, cartographie, analyse du trafic des sites web, stockage de blogs, de photos, de vidéos, de livres... L'entreprise Google s'est diversifiée et les questions auxquelles elle est confrontée également.

En plus de la recherche d'informations, Google offre aux internautes de nombreux services en ligne "gratuits" qui sont rémunérés grâce à la publicité à laquelle ils sont associés. Le recours à ces services peut porter atteinte à la vie privée des internautes, du fait justement des publicités ciblées qui les accompagnent.

Le service de messagerie Gmail

La messagerie Gmail analyse le contenu des messages envoyés et reçus afin d'insérer dans son interface des liens publicitaires personnalisés. Cette analyse se heurte notamment au droit français et européen concernant le secret des correspondances privées. Le consortium Privacy International a ainsi déposé une plainte dans 15 pays contre Gmail pour, entre autres, non-respect des