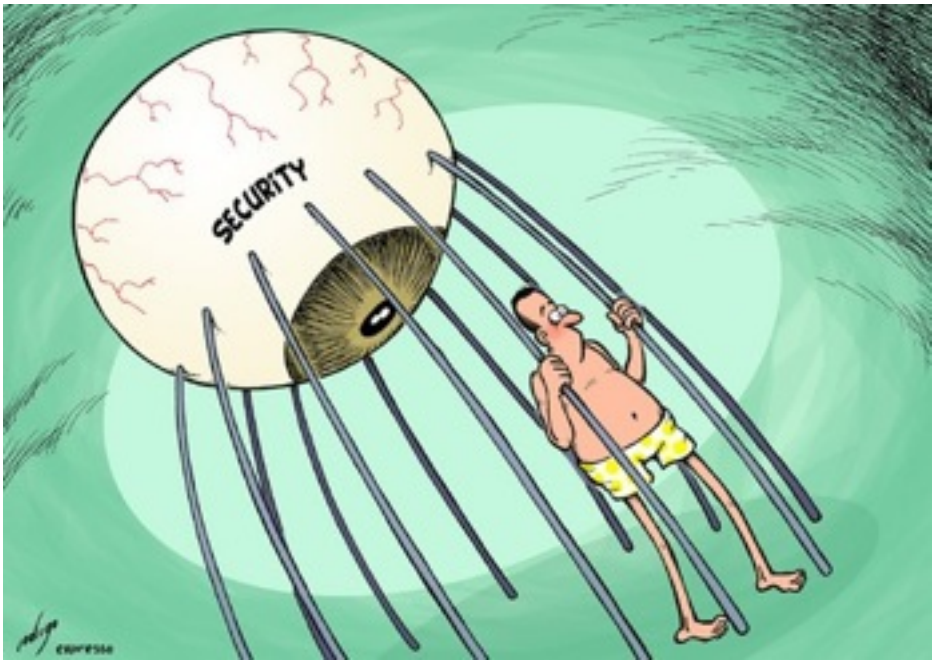
Big Data: Big Brother or Big Friend ?

A l'ère Post Snowden et du développement des outils numériques, doit-on craindre pour nos libertés ?



Objets et jeux connectés, activités sur les réseaux sociaux, géolocalisation sur les smartphones, requêtes sur les moteurs de recherche; des milliards de données transitent dans la sphère numérique.

Regroupées, traitées, triées, analysées, ces informations constituent notre e-profil, dont nous ne maitrisons ni le contenu, ni l'utilisation.

L'explosion d'Internet et la création de nouvelles e-technologies ont permis le développement de nouveaux modes de surveillances, un regard invisible dont nous ne soupçonnons pas la menace.

En exploitant nos peurs et l'insécurité qui règne face à la monté du terrorisme, certains tentent de justifier le bien fondé de ces nouvelles pratiques attentatoires à nos libertés.

La lutte contre la criminalité ne doit pas sacrifier la préservation de nos libertés fondamentales et notamment celles de pouvoir garder une main mise sur nos informations personnelles et notre intimité.

Il s'agit donc, pour nos pouvoirs public et autres sociétés privées, de trouver un compromis entre les intérêts économiques, diplomatiques et sécuritaires qu'ils défendent et le droit fondamental de disposer d'une vie privée.

Afin que chacun prenne conscience du risque lié aux dérives de cette surveillance, faut-il encore mesurer l'ampleur de ces pratiques et la dimension qu'elles prennent dans notre quotidien.

Jusqu'où s'étend la surveillance ?

Le phénomène de surveillance massive apparu au début des années 2000 est largement né outre atlantique, aux Etats Unis, dans un climat de guerre et de lutter contre le terrorisme.

Les prémices d'une surveillance de masse…

Au lendemain du 11 septembre 2001, la priorité était donnée à la sécurité et à la lutte contre le terrorisme.
Le Président Bush s'empressa, dès le 26 octobre 2001, de signer le « **Patriot Act** », dite « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ».
Cette loi liberticide, votée dans l'urgence et dans un climat de paranoïa collective, autorise purement et simplement les agences de sécurité américaine à surveiller la circulation des messages électroniques et à conserver les traces de la navigation sur le Web de toute personne suspectée de contact avec une puissance étrangère.
Elle permettait également à la NSA (National Security Agence), la mise sur écoute de toute personne ayant un rapport proche ou lointain avec une personne présumée terroriste.
L'explosion parallèle de l'utilisation d'internet et des téléphones portables comme moyen de communication, a renforcé les missions de la NSA.
La NSA devenait alors un pilier du renseignement et de l'espionnage américain.

Portée par la traque d'actes terroristes et d'Al Qaïda, la **NSA** ne se limitait cependant pas à luter contre les acteurs de cette « guerre de terreur » et n'hésitait pas à agir en dehors du cadre purement sécuritaire.
Le 6 juin 2013, Edward Snowden, ancien agent de la NSA, révélait au monde entier, des documents secret témoignant de l'existence de vastes opérations d'écoutes et de surveillance menées par l'agence.
La NSA n'a cessé de collecter et stocker des milliards de données de communication et de connexion afin de garder une main mise totale sur les comportements.

Disposant de larges pouvoirs d'intervention, la NSA enjoignait les opérateurs de téléphonie et les moteurs de recherche, à lui communiquer les données et informations de leurs utilisateurs.
L'agence a développé également une méthode d'interception directe des conversations et des données sur les réseaux liant les serveurs aux opérateurs et aux moteurs de recherche.
Les documents rendus public par Edward Snowden et relayés par de nombreux médias, ont révélés l'existence d'opérations ayant pour cible, des acteurs économiques et politiques du monde entier, hostiles ou non aux Etats-Unis.
Les Présidents français, Jacques Chirac, Nicolas Sarkozy et François Hollande et d'autres dirigeants de pays alliés, ont été surveillés et espionnés téléphoniquement par la NSA.
Ces récentes révélations ont fait l'effet d'une bombe mais ont permis de mettre en lumière l'ampleur de la surveillance menée par les Etats Unis et les pratiques totalement déloyales et illégales utilisées par la NSA.

Par décision en date du 7 mai 2015, la Cour d'Appel fédérale a déclaré **illégales et anticonstitutionnelles** les pratiques de la NSA consistant à collecter et stocker des données de communications téléphoniques de

millions d'américains, et menées sur la fondement de la section 215 du Patriot Act.
Cette dernière disposition n'ayant plus d'effet juridique au 1er juin 2015, la décision de la Cour d'Appel fédérale n'a qu'une portée symbolique.
Elle sert cependant d'argument contre le vote d'une loi de reconduction pure et simple du Patriot Act, sans modifications et renouvelant le dispositif de surveillance tant critiqué.
Le « USA Freedom Act » a finalement été voté par le Congrès, le 3 juin 2015, mais n'a pas renouvelé la disposition 215 litigieuse.
La NSA ne pourra désormais accéder aux données téléphoniques stockées par les opérateurs eux même, que sur demande précise visant des cibles identifiées ou leur entourage, lesquelles devront être autorisées par une cour fédérale américaine.

Cette psychose sécuritaire n'a pas seulement touché les autorités publiques. De nombreuses initiatives citoyennes, toujours plus intrusives et attentatoires à nos libertés, ont vu le jour.
Le projet dit NOLA, initié à la Nouvelle Orléans, met en place un système de vidéo surveillance communautaire privé, lequel autorise chaque citoyen à placer des caméras dans leur propriété. Ces vidéos convergent directement vers un centre de traitement, via Internet.
Les enregistrements permettent ensuite aux services de police d'identifier les auteurs d'infractions et constituer des preuves devant une cour de justice.

La montée de la suspicion et l'obsession de l'anticipation a atteint son plus haut degré à Santa Cruz, en Californie, où le programme informatique **PRED POL** (Predicitv policing) a été expérimenté.
Ce logiciel est un algorithme conçu pour prédire la période de la journée, et l'endroit de la ville où il existe un risque élevé qu'un crime soit commis, afin de renforcer les effectifs policier.
Cette approche scientifique utilise les données recensant les infractions passées et permet d'orienter précisément les interventions des agents de police.

En dehors de tout enjeu sécuritaire et dans un but purement économique, cette surveillance à grande échelle des moyens de communication privée, permet d'avoir une connaissance profonde des consommateurs.
Les informations et données affichées et communiquées sur les réseaux sociaux, sont classées et analysées pour constituer notre e-profil.
Les données collectées permettent d'identifier notre caractère, nos envies, notre état d'esprit, et ainsi influencer notre pouvoir d'achat.
Le réseau social, Facebook, vend ses bases de données en proposant ainsi aux entreprises, une publicité personnalisée et ciblée.

Un oeil sur les français…

Suivant le chemin des Etats-Unis, La France n'a eu de cesse, ces dix dernières années, de renforcer son arsenal législatif sécuritaire et les pouvoirs de surveillance de ses autorités.

Le 10 décembre 2013, a été voté la **loi de programmation militaire** (LPM) pour les années 2014 à 2019 élargissant les moyens d'action des pouvoirs publics en matière de collecte de données.
Elle permet entre autre, le recueil auprès d'opérateurs de communication électronique, d'informations et de documents, traités et conservés par eux.
Il ne s'agit donc plus seulement de collecter des données de connexion, ou métadonnées, qui n'informeraient que sur la localité, la date, et l'identité des appels téléphoniques. Désormais, le ministère de l'économie et du budget pourra requérir l'interception ou la capture « d'informations ou documents traités ou conservés par leurs réseaux ou services ».
Enfin, les finalités de ces mesures ne se limitent plus qu'à la prévention du terrorisme mais aussi à la sauvegarde du *« potentiel scientifique et économique de la France »* et à la prévention *« de la criminalité ou de la délinquance organisée ».*
Le texte a emporté de vives critiques de la part de trois associations de défense des libertés numériques (Quadrature du net, French Data Network, et la fédération des fournisseurs d'accès associatif français) lesquelles ont déposé une question prioritaire de constitutionnalité (QPC) devant le Conseil d'Etat, transmise au Conseil Constitutionnel, le 5 juin 2015.

Ce dernier texte à peine promulgué, une nouvelle **loi anti-terroriste** a été votée, le 13 novembre 2014, prévoyant, outre, la possibilité de bloquer administrativement et sans autorisation judiciaire, le contenu d'un site internet, le renforcement des moyens numériques d'investigation de la police.
Elle permet désormais aux enquêteurs de procéder à une perquisition sur les systèmes informatiques « distant » et accéder aux données stockées dans lesdits systèmes, directement depuis les locaux de leurs propres services, sans devoir se rendre sur les lieux.

Les nombreuses protestations d'associations de défense des libertés, de syndicats professionnels, de médias et de personnalités publiques, mettant en garde les parlementaires et le gouvernement sur l'atteinte disproportionnée que cette surveillance légalisée pourrait avoir sur nos libertés, ont été vaines.

Au lendemain des attentats de Paris en janvier 2015, l'émotion a rapidement fait place à la précipitation et à la nécessité de légiférer et renforcer le dispositif de surveillance à la disposition des services de police.
Le projet de **loi de renseignement**, en préparation depuis deux ans, a été présenté en urgence en Conseil des ministres le 19 mars 2015.
Le texte a pour but de légaliser et encadrer les pratiques existantes d'écoute, mais également doter les services de sécurité d'outils et de méthodes de surveillance plus adaptées.

Le cadre et les finalités de la loi sont énumérés à l'article 811-3 du Code de la sécurité intérieure. Le recours aux techniques prévues par la loi a pour but « *la promotion des intérêts fondamentaux de la Nation* » suivants:

- 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements

européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
- 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
- 4° La prévention du terrorisme ;
- 5° La prévention : *a)* Des atteintes à la forme républicaine des institutions ; *b)* Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; *c)* Des violences collectives de nature à porter gravement atteinte à la paix publique ;
- 6° La prévention de la criminalité et de la délinquance organisées ;
- 7°La prévention de la prolifération des armes de destruction massive.

A la lecture de ces « intérêts publics » justifiant le recueil de renseignements, il apparait clairement qu'il ne s'agit pas exclusivement de lutter contre une menace terroriste.
La nécessité de prévenir « *des violences collectives de nature à porter gravement atteinte à la paix publique* » fait directement référence à la surveillance de mouvements sociaux, ou de catégories entières de la population.
Les ingérences aux libertés fondamentales prévues par la loi sont telles, que la loi aurait dû user de termes précis, clairs, et circonstanciés afin de garantir la proportionnalité et la nécessité des dispositifs attentatoires mis en oeuvre.
En ne définissant pas chaque motif d'intérêt public de manière précise et restrictive, la loi ouvre la porte aux abus.
Le texte offre un cadre très large aux actions des services de renseignement, favorisant davantage une approche offensive que préventive.

La loi offre ainsi aux agents du renseignement, un large **panel de dispositifs techniques d'écoute et de surveillance.**

Les réquisitions administratives d'informations auprès des opérateurs de téléphonie, déjà autorisées par la loi de programmation militaire, pourront désormais être effectuées individuellement et en temps réel.
La mise en oeuvre de traitements automatisés sur les réseaux desdits opérateurs pourra leur être imposée afin de détecter des connexions susceptibles de révéler une menace terroriste, mais en ne permettant pas, précise le texte, d'identifier les personnes auxquelles les informations se rapportent.
Pour ce faire, la pose de dispositifs techniques, communément appelés « boites noires », sur les réseaux, afin de détecter des potentielles menaces à travers une analyse des métadonnées, sera autorisée.
Ces métadonnées ne révèlent aucun contenu, mais renseignent précisément sur le lieu, la date et l'identité de l'expéditeur et des destinataires des informations interceptées.
Ces données techniques relatives à la localisation des équipements terminaux utilisés pourront être recueillies sur sollicitation du réseau et transmises en temps réel par les opérateurs aux agents.

Mais le texte va plus loin en permettant aux services de renseignement de recueillir directement ces métadonnées au moyen de dispositifs spéciaux de captation désormais autorisés.

Le texte prévoit en effet de légaliser l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule, ou d'un objet.
Des agents spécialement habilités pourront s'introduire dans un véhicule, un lieu privé ou

un système automatisé de traitement de données.

Le texte autorise enfin l'utilisation de dispositifs techniques permettant « *les interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements entrant dans les finalités de la loi* ».

Ces dispositifs techniques, permettront de capter, fixer, transmettre et enregistrer des paroles prononcées, à titre privé ou confidentiel, ou d'images dans un lieu privé, mais également des données informatiques transitant par un système automatisé de données, ou contenues dans un tel système.

La pose de micros et de caméras espions est donc autorisée, comme l'utilisation de « keylogger », ces logiciels qui peuvent lire et enregistrer en temps réel ce qu'un utilisateur tape sur le clavier.
Des balises de géolocalisation et des « IMSI-Catchers » pourront également être utilisées. Ces appareils espions peuvent capter toutes les communications dans un périmètre donné, celle du suspect poursuivi mais aussi celles de toutes les personnes se trouvant dans le voisinage.

Porté, défendu et amendé par le député Jean-Jacques Urvoas, le texte a été largement **critiqué** en ce qu'il permet l'utilisation de techniques attentatoires aux libertés publiques, sans véritables garanties, ni contrôle proportionné.

Selon le Conseil National du Numérique, le dispositif de détection automatisée sans identification des personnes auxquelles les informations se rapportent, est indéniablement un mode de collecte qui confine à une forme de surveillance généralisée et indiscriminée des réseaux.

L'organe chargé de contrôler les pratiques de surveillance est la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui remplace l'ancienne autorité chargée d'autoriser les écoutes administratives, la Commission nationale de contrôle des interceptions de sécurité (CNCIS).
La loi prévoit que la CNCTR devra obligatoirement être consultée pour avis avant la mise en oeuvre des techniques de recueil d'informations.
Cet avis n'est, cependant, que consultatif, dès lors que le Premier Ministre pourra autoriser la mise en oeuvre d'un dispositif, malgré le refus de la CNCTR. La procédure dans ce cas prévoit la possibilité de saisir le Conseil d'Etat, mais à des conditions très strictes.
Ce contrôle a priori n'est en outre pas systématique, puisque le texte voté prévoit une procédure d'urgence sans avis préalable de la CNCTR, laquelle doit simplement être informée.
L'absence de contrôle efficace en amont fragilise davantage la protection des libertés poursuivies par le législateur.

En outre, le défenseur des droits de l'Homme a mis l'accent sur l'absence de garanties supplémentaires effectives pour les avocats tenus au respect du secret professionnel et occupant une place centrale dans l'administration judiciaire.
En effet avant de rappeler qu'un avocat « *ne peut être l'objet d'une demande de mise en œuvre d'une technique de recueil de renseignement à raison de l'exercice de son mandat ou de sa profession* », le texte ajoute que lorsqu'une telle demande « *concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle*

des techniques de renseignement est examiné en formation plénière. »
Aucunes garanties particulières ne sont ainsi mise en place, là où un contrôle judiciaire et, à tout le moins, du bâtonnier de l'ordre des avocats, aurait été plus opportun.

Outre des garanties contre des abus amoindris, le texte reste flou sur certains points sensibles.
La loi ne prévoit pas à quel moment la judiciairisation, c'est à dire le passage de la phase de police administrative à la phase judiciaire, doit intervenir.
Si la finalité de la police administrative reste préventive, elle ne l'est plus lorsqu'il s'agit de rechercher et de poursuivre les preuves d'une infraction.
Ces missions devant être menées dans le cadre d'une enquête de police judiciaire, la loi aurait dû prévoir les critères objectifs d'engagement de la procédure judiciaire.
Le recueil d'informations collectées pose également une autre difficulté liée aux éléments de preuve qu'elles contiennent.
En effet, si les éléments collectés constituaient des preuves dans le cadre d'une procédure pénale qui serait ouverte, le texte ne précise pas si l'auteur présumé ou son représentant pourrait avoir accès à ces données, dans le respect du principe du contradictoire et des droits de la défense.
La loi n'accorde pas non plus à une personne incriminée sur le fondement d'éléments ainsi collectés, du droit de disposer d'un recours effectif pour contester la régularité ou la légalité d'un dispositif de surveillance mis en oeuvre à son encontre.

Ces critiques n'ont cependant pas freiné le processus d'**adoption** du texte, qui a été voté le 24 juin 2015, à l'assemblée nationale, par une large majorité.

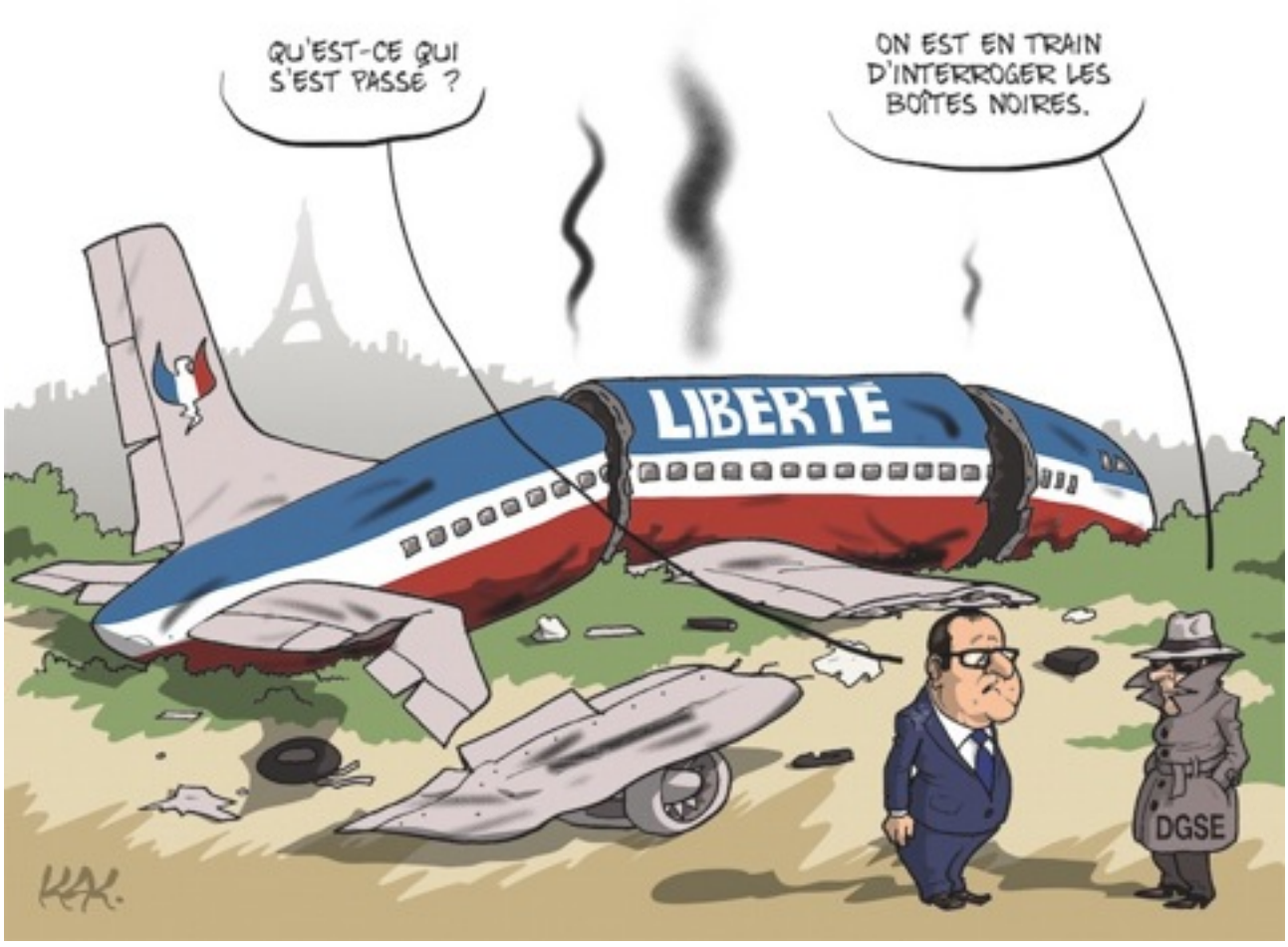
Les récentes révélations sur les écoutes pratiquées par la NSA n'ont pas non plus dissuadé les parlementaires, allant même jusqu'à affirmer qu'elles devaient justifier le renforcement des services de renseignement et de contre-espionnage.

Saisi par le Président de la République, et plus de 60 députés, le **Conseil Constitutionnel** s'est prononcé, le 23 juillet 2015 sur la conformité du texte à la Constitution.
Les nombreux griefs soulevés contre les dispositions de ce texte, n'ont cependant pas justifié une large censure de la loi.
Seules les dispositions sur la procédure d'urgence opérationnelle justifiant l'absence de délivrance préalable d'une autorisation du Premier ministre et d'un avis préalable de la commission nationale de contrôle des techniques de renseignement, ont été censurées. Cette procédure portait une atteinte manifestement disproportionnée au respect de la vie privée et au secret des correspondances.
Pour le reste, le traitement automatisé des données de connexion, l'utilisation de dispositifs techniques permettant la captation de conversations et de données informatiques sont conformes, à condition, précise le Conseil Constitutionnel, que la mesure soit proportionnée à la finalité poursuivie et aux motifs invoqués.
Les espoirs des défenseurs d'un droit au respect de la liberté numérique, ont été anéantis et devront l'être davantage, si les autres réformes envisagées étaient adoptées.

Au delà du territoire national, la mise en oeuvre d'un système de surveillance au niveau européen a également été proposé à travers la création d'un système européen dit **PNR** (Passenger Name Record).
Les PNR sont l'ensemble des informations collectées auprès des passagers aériens au stade

de la réservation commerciale. Elles permettent d'identifier l'itinéraire de déplacement, les vols concernés, le contact à terre du passager, les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que les préférences alimentaires spécifiques.
Ce système existe déjà en France depuis la loi anti terroriste du 23 janvier 2006, mais reste limité à quelques pays extérieurs n'appartenant pas à l'Union Européenne, dès lors que les vols intracommunautaires sont exclus de ce dispositif.
La mise en place d'un système PNR au niveau européen permettrait de centraliser toutes les informations relatives aux passagers des vols en provenance et à destination d'un pays de l'Union européenne.
L'Union européenne se refuse, cependant, à ce jour, de voter favorablement un tel dispositif, jugé excessivement attentatoire au droit à la protection de la vie privée.

Ces nouvelles dispositions législatives adoptées ou envisagées offrant un cadre légal aux programmes de surveillance de masse, doivent nécessairement être accompagnées d'un arsenal législatif de protection des données personnelles.
Si des dispositifs de contrôle existent déjà, il faut impérativement envisager de les renforcer et les adapter aux nouveaux enjeux actuels.



Quelle protection contre la surveillance ?

La protection des données à caractère personnel est un droit fondamental, garanti par un cadre juridique national et européen.
L'explosion de l'utilisation d'internet impose d'adapter et de perfectionner les outils de protection existant afin d'éviter tout mauvais usage de la surveillance vidéo, des étiquettes d'identification par radiofréquence (puces intelligentes), de la publicité comportementale, des moteurs de recherche et des réseaux sociaux.

Au niveau européen, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne considèrent le respect de la vie privée et la protection des données à caractère personnel comme des droits fondamentaux étroitement liés, mais distincts.
Le droit à la protection des données est autonome du droit à la vie privée et fait référence à un espace intermédiaire d'exposition plus ou moins maitrisé, ni totalement privé, ni totalement public.
La charte est intégrée au Traité de Lisbonne et revêt un caractère juridiquement contraignant pour les institutions et les organes de l'Union européenne.

Différents instruments législatifs de l'Union européenne sont en vigueur mais aucun régime unique n'existe. Parmi ces textes, la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, est le principal outil de protection. Cette directive établit des conditions générales de licéité des traitements de données personnelles ainsi que les droits des personnes concernées. Elle prévoit l'établissement d'autorités indépendantes de contrôle dans les États membres. Le traitement de données à caractère personnel n'est ainsi autorisé que si la personne concernée a donné son consentement explicite à un tel traitement et qu'elle en a été préalablement informée.
Créée avant l'utilisation massive d'internet, la directive a permis, sous quelques mesures, de faire face au développement des réseaux sociaux. Il reste cependant que les mesures mises en place par ce texte n'apportent pas de solutions adaptées aux problématiques actuelles.
Les mesures permettant de sanctionner des manquements à cette directive étant nationales, aucune réponse unique ne peut être apportée.

Un nouveau cadre juridique global sur la protection des données au niveau de l'Union européenne fait actuellement l'objet de discussions.
Le 25 janvier 2012, la Commission a proposé l'adoption de nouvelles mesures législatives visant à réformer la législation de l'Union sur la protection des données. Cette proposition a pour but de garantir la protection des données à caractère personnel dans l'ensemble de l'Union, d'accroître le contrôle des utilisateurs sur leurs propres données et de réduire les coûts pour les entreprises.
Les évolutions technologiques et la mondialisation ont profondément modifié les modes de collecte, d'obtention et d'utilisation des données.

L'adoption d'une législation unique permettra de mettre fin à la fragmentation actuelle. La présente initiative contribuera au renforcement de la confiance des consommateurs dans les services en ligne et à l'indispensable relance de

la croissance, de l'emploi et de l'innovation en Europe.
Une proposition de règlement général visant à actualiser les principes ancrés dans la directive de 1995 sur la protection des données, permettra de passer d'une logique de formalité procédurale à une logique de conformité substantielle en matière de protection des données.
Les acteurs du traitement de données à caractère personnel ne devront plus solliciter l'autorisation d'utiliser ces données auprès des autorités nationales compétentes, puisque ces dernières devront les accompagner et leur apporter une double expertise juridique et technique.
En outre, dès lors que les données ne connaissent pas de frontière, le règlement prévoit de créer une procédure unique, afin d'apporter une réponse unique au sein du territoire de l'Union européenne. Les entreprises pourront s'adresser à l'autorité indépendante d'un pays membre de l'Union, « guichet unique », à charge pour elle de coopérer avec les institutions des autres pays et permettre d'uniformiser les solutions.
Le Parlement et le Conseil examinent actuellement les propositions de la Commission.

Comblant les lacunes de la directive du 24 octobre 1995, et anticipant sur le prochain règlement à intervenir, la jurisprudence de l'Union européenne a sanctionné des atteintes à la protection des données personnelles à travers des droits qu'elle découvre.
C'est ainsi que dans une décision du 13 mai 2014 et suivant un raisonnement méthodique, la Cour de Justice de l'Union Européenne (CJUE) a consacré le droit à l'oubli.
Il s'agissait de déterminer si le moteur de recherche Google effectuait un traitement de données à caractère personnel, pour déterminer si le déréférencement d'une information périmée devait leur être imposé.
La CJUE estime dans un premier temps qu'en recherchant de manière automatisée, constante et systématique des informations publiées sur Internet, Google procède à une « collecte » des données au sens de la directive. L'exploitant du moteur de recherche est le « responsable » de ce traitement, au sens de la directive, étant donné qu'il en détermine les finalités et les moyens.
Selon la Cour ces informations pouvaient potentiellement révéler une multitude d'aspects de la vie privée, de sorte qu'un profil plus ou moins détaillé des personnes recherchées pouvait être établi. Une telle ingérence ne saurait être justifiée par le seul intérêt économique de l'exploitant du moteur dans le traitement des données.
La Cour constate qu'il y a lieu de rechercher un juste équilibre entre les nécessités du droit à l'information et le droit au respect de la vie privée et aux données à caractère personnel.
C'est dans ces conditions que la Cour relève que la directive 95/46/CE permet à tout individu de solliciter la suppression des liens vers des pages web contenant les informations relatives à sa personne.

La CJUE contrôle également la conformité des normes communautaires aux principes qu'elle garantit. C'est ainsi, que par un arrêt du 8 avril 2014, la CJUE a invalidé la directive du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public pour lutter contre le crime organisé et le terrorisme.
Le texte prévoyait l'obligation pour les fournisseurs de services de télécommunications de conserver, pendant un délai de six à vingt-quatre mois, les données relatives au trafic et à la localisation des interlocuteurs. La CJUE a

relevé dans un premier temps que ces données étaient susceptibles de fournir des indications très précises sur la vie privée des personnes dont les données sont conservées, et constituait ainsi une ingérence grave à l'exercice des droits et libertés garantis.
Une telle conservation de données, couvrant l'ensemble des abonnés et utilisateurs européens, n'était pas justifiée, ni proportionnée à l'objectif poursuivi. L'absence de contrôle effectif contre les risques d'abus et de dispositions imposant la conservation de ces données sur le territoire de l'Union européenne constituaient une violation de la directive de 95/46 sur le traitement des données à caractère personnel.
La condamnation de ce texte par la CJUE laisse présager une position similaire concernant la loi de renseignement promulguée en France le 24 juillet 2015.
Dans une lettre du 17 juin 2015, la commission de Bruxelles avait déjà pointé du doigt le projet de loi sur le renseignement, lequel ne garantissait pas, face au renforcement des pratiques de renseignement, « *un contrôle judiciaire et démocratique suffisant* ».

En France, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, transposant la directive communautaire du 24 octobre 1995, fixe les conditions de liciété des traitements de données personnelles et les obligations incombant aux responsables de ce traitement. Le contrôle de la mise en oeuvre du traitement de ces données est assuré par la Commission nationale de l'informatique et des libertés (CNIL).
Au titre de ses missions, cette autorité administrative indépendante accorde les autorisations nécessaires, établit des normes, reçoit des réclamations et plaintes, et émet des avis relatifs à la mise en oeuvre des traitements des données personnelles.
C'est ainsi qu'à la suite de contrôles effectués auprès de plusieurs sites de rencontre ayant révélé de nombreux manquements à la loi Informatique et Libertés, la CNIL a mis en demeure, le 24 juin 2015, huit acteurs du secteur, de se mettre en conformité avec la loi.
Il leur a été reproché de ne pas recueillir le consentement exprès des personnes concernant la collecte de données sensibles relatives à la vie et aux pratiques sexuelles, aux origines ethniques, aux convictions et pratiques religieuses et aux opinions politiques.
Les sites ne procèdent pas non plus à la suppression des données des membres ayant demandé leur désinscription ou ayant cessé d'utiliser leurs comptes depuis une longue durée.

Afin de garantir l'application effective des dispositions de la loi du 6 janvier 1978, la CNIL dispose également d'un pouvoir de sanction pécuniaire, d'injonction de cesser les traitements de données, et de retrait de l'autorisation accordée.

Faisant une application directe de la jurisprudence européenne consacrant le droit à l'oubli, les juges du fond contrôle également l'application de la loi du 6 janvier 1978.
C'est ainsi que par une décision du 9 décembre 2014, le TGI de Paris a précisé les conditions d'application du droit au déréférencement.
Les données qui ne seraient pas pertinentes au regard des finalités du fichier, au sens de l'article 6 c) de la loi, doivent ainsi être rendues non visibles par le moteur de recherche. Les critères du caractère pertinent tiennent à la nature des données conservées, aux motifs de la demande, et au temps écoulé entre les faits et la demande de déréférencement.

Le moteur de recherche avait donc été condamné à déréférencer les données relatives à la condamnation pénale de l'intéressé qui avaient été effacées de son casier judiciaire depuis plus de huit ans et dont la visibilité sur internet nuisait à sa recherche d'emploi.
Depuis l'arrêt de la CJUE du 8 avril 2014, Google reçoit plus de 1000 demandes quotidiennes de déréférencement provenant de français.

S'il parait impossible de freiner ce processus de surveillance de masse, une **alternative** consisterait à permettre à chacun de contrôler la communication de ses données personnelles.
Une expérience d'optimisation du partage des données a été effectuée à Trendt, une ville au nord de l'Italie. Chaque citoyen possédait une boite personnelle, et décidait librement du contenu des informations qu'ils partageaient dans l'espace de réseau (cloud) crée. Aucune donnée ne leur échappait dès lors que le cloud permettait de déterminer l'identité de ceux qui utilisaient les informations partagées.
La généralisation d'une telle utilisation des données à caractère personnel serait appréciable en ce qu'elle favoriserait un système d'entraide et de partage en toute transparence.

Directrice de publication: Celia Boukhtouche
Sources:
- www.mediapart.fr
- www.cnil.fr
- www.legifrance.fr
- www.curia.europa.eu
- Conférence de M. Geffray, Secrétaire général de la CNIL