L’identité numérique et la protection des données personnelles

Qu’est-ce que la veille juridique ?

Au sens large, la **veille juridique** est une veille orientée dans le domaine du droit. Elle concerne essentiellement les lois, les décrets ou tout type d’objets juridique qui traite un sujet du droit.

La veille juridique consiste donc pour un individu ou une organisation à :

- **Identifier** à travers différentes sources d’informations sélectionnées, toute nouvelle disposition juridique ou texte de droit ;
- **Traiter** cette information en lui donnant une pertinence juridique ;
- **Diffuser** cette information à son demandeur sur tout type de support adapté à ce dernier (papier, document, Internet, journaux …)

L'identité numérique - Définition :

Elle est définie comme un lien technologique entre une entité réelle (une personne) et une entité virtuelle (sa représentation numérique).

L'entité réelle peut-être donc un utilisateur d'Internet par exemple et son entité virtuelle est un avatar posté sur Twitter par exemple, afin de s'identifier en tant qu'utilisateur sur Twitter.

Internet étant accessible par tous et offrant de plus en plus de services, se pose le problème de la sécurité de l'information et plus particulièrement des données personnelles. La gestion de l'identité numérique devient alors un enjeu majeur.

L'identité numérique en Droit :

Principe du droit à l'image sur Internet :

En France, la loi comporte aujourd'hui plusieurs textes pour protéger l'image des personnes ou des entreprises.

> **Article 9 :**
>
> ***« Chacun a droit au respect de sa vie privée.***
>
> ***Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »***

Ce même article définit également le **respect de la vie privée sur Internet**.

En France, un projet gouvernemental a été mise en place en faveur d'une signature numérique sécurisé afin d'identifier virtuellement le citoyen français :

- En mars 2011, une nouvelle a été promulguée et proposé par l'ancien Premier Ministre François Fillon, il s'agi de la réforme de l'ancienne loi dite LOI LOPPSI, la **LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.**

  Cette loi fonctionne théoriquement contre les spams et l'hameçonnage, il prévoit d'autres mesures :

  Notamment le **filtrage** qui permettra aux autorités administratives de bloquer les sites jugés pédopornographiques (la liste devra rester confidentielle) ….

- En mars 2012, le gouvernement Fillon a promulgué et fait voter la loi de la protection de l'identité numérique. La **LOI n° 2012-410 du 27 mars 2012** relative à la protection de l'identité est explicite, et ce, dès le premier article :

> **Article 1 :**
> ***« L'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier. »***

Le second article défini ensuite de quoi une carte d'identité et un passeport est composée :

> **Article 2 (extrait) :**
>
> ***« La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :***
> ***1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;***
> ***2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;***
> ***3° Son domicile ….. »***

L'objectif de cette lois et de garantir la fiabilité maximale aux passeports et aux cartes nationales d'identité, afin de luter conte les délits liés à l'usurpation d'identité et à la fraude documentaire.

En cas d'usurpation d'identité, que dit le code pénal ?

> **Article 226-4-1 (extrait) :**
>
> ***« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. »***

Cet article a été mis à jour dans le cade de la **LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure** dite **LOI LOPPSI 2** proposé par le gouvernement Fillon qui réforme l'ancienne **LOI n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure** dite **LOI LOPPSI.**

Notez que l'usurpation est aussi directement sanctionnée dans un autre cas : **le fait de prendre le nom d'un tiers**. En effet, l'article 434-23 du Code Pénal puni :

> **Article 434-23 (extrait) :**
>
> ***« Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. »***

Autre projet annoncé par le gouvernement Fillon il y a un an, baptisé **Idénum**, il s'agit d'un projet imaginé par NKM à l'époque ministre de l'économie numérique, puis repris par Fleur Pèlerin en Janvier 2013, l'objectif de ce projet est de créer un label qui certifiera que cet identifiant permet bien de récupérer des données qualifiées suffisantes pour s'identifier à un autre service, à l'image de Facebook, sauf que ce dernier n'est ni sécurisé, ni de garanti d'identité.

---

1) Les données personnelles : principes et droits :

Plusieurs organismes ont définies les données personnelles, mais toutes les définitions ont la même signification.

a) Les données personnelles – Définition générale :

Ce sont les informations qui permettent d'identifier directement ou indirectement une personne physique.

Les données personnelles aujourd'hui correspondent essentiellement au nom, prénom, adresse, courriel, âge, date de naissance. Cela peut être également des informations professionnelles comme le numéro de la sécurité sociale, la carte de crédit, une photo, une emprunte digital. Grâce à Internet, il est possible de rechercher une personne avec son nom/prénom par l'intermédiaire d'un moteur de recherche (Google ou Qwant), c'est d'autant plus vrai sur les réseaux sociaux où il est facile de chercher la/les personnes que l'on veut savoir.

b) La loi « Informatique et Libertés », qu'est-ce que c'est ?

Il s'agit d'une loi qui traite et décrit des règles dans le domaine de l'informatique, il a été promulguée et appliquer le 6 Janvier 1978 par le président de la République de l'époque, à savoir Giscard d'Estaing, par la suite, une Commission a été mise en place la même année afin de proposer des « mesures tendant à garantir que le développement de l'informatique se réaliserait dans le respect de la vie privée et des libertés individuelles et publiques ». Les travaux de cette Commission ont conduit à l'adoption de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et à l'institution de la CNIL comme organisme chargé de veiller à l'application de ce texte.

c) Qu'est-ce que la CNIL ?

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante composée de 17 membres (parlementaires, hauts fonctionnaires, magistrats, personnalités qualifies.

Elle dispose de son propre budget. La Commission est chargée de veiller à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Informatique et Libertés : Les principes – Section I Chapitre 1 :

La loi historiquement a été découpée en treize parties, et les 3 premiers articles concernent directement les citoyens français. Dès le premier article, la CNIL inscrit l'informatique dans le cadre des droits de l'homme, certainement en souvenir des détournements qu'ont pu subir les informations personnelles durant le nazisme.

Article 1

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

En lisant le second article, la loi décrit son cadre, s'adressant aux plus grand nombre (organisme compétent par exemple) :

Article 2 (extrait)

« [...] Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne… »

Notez que cette article définis de manière juridique ce qu'est une données personnelle, c'est le point de vue de la CNIL.

La loi défini ensuite quelles sont les obligations d'un responsable de traitement et quels peuvent-être les destinataires de ce traitement :

Article 3 (extrait)

« Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. »

Notez que l'article 3 décrit aussi le droit d'information, en effet, ce dernier indique que toute personne a le droit de savoir si elle est fichée et, si oui, dans quel fichier, c'est ce qu'on appelle le droit d'information, droit fondamental base de tous les autres.

Informatique et Libertés : Les conditions de traitement des données à caractère personnelles – Section II Chapitre 1 :

La seconde partie de la loi décrit de manière précise comment les données à caractère personnelles doivent être récoltés et conservées, qui sont les acteurs légitimes du traitement, et ce, dès l'article 6 et 7, l'article 6 décrit aussi juridiquement le **respect de la vie privée sur Internet** :

Article 6 (extrait)

« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :
***1°** Les données sont collectées et traitées de manière loyale et licite ;*

***2°** Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalité…*

Article 7 (extrait)

« Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :
1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée … »

Informatique et Libertés : Disposition propres à certaines catégories de données – Section 1 Chapitre II :

Enfin dans les articles 9 et 10, elle précise que seules les juridictions, autorités publiques, personnes gérantes d'un service public ou auxiliaire de loi peuvent mettre en œuvre des traitements de données relatifs aux infractions, condamnation et mesure de sûreté et qu'aucune décision de justice ou

impliquant des conséquences juridiques ne peut être basée sur un traitement de données à caractère personnel, protégeant ainsi les personnes de toute malversation.

Article 9 (extrait)

« Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :
***1°** Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;*

***2°** Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ; …. »*

Article 10 (extrait)

« Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité … »

d) Les droits reconnus par la loi et la CNIL :

Parmi les 7 principes que la CNIL a décrit et reconnaît, un seul attribue des droits pour les citoyens, il s'agit du principe du droit des personnes, c'est la plus importante puisqu'il décrit certains droits reconnu par la loi que les citoyens peuvent saisir et revendiquer, surtout quand ils se sentent en danger quant à leurs données personnelles :

7.1 : Informer les intéressés :

Lors de l'informatisation de tel ou tel service, ou lorsque des données sont recueillies par exemple par voie de questionnaires, les usagers concernés et le personnel de l'organisme doivent être informés de la finalité du traitement, du caractère obligatoire ou facultatif du recueil, des destinataires des données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi "Informatique et Libertés" : **Il s'agit droit d'accès et de rectification mais aussi, droit de s'opposer, sous certaines conditions, à l'utilisation de leurs données.**

7.2 : Droits d'accès et de rectification :

Les citoyens peuvent demander la communication de toutes les informations les concernant contenues dans un fichier détenu par l'établissement et ont la possibilité de faire rectifier ou supprimer les informations erronées.

Deux articles ont été par ailleurs définis concernant d'une part le droit d'accès à ses données personnelles, et le droit de rectification de ses données d'autre part :

Article 39 sur le droit d'accès :

« Toute personne a le droit d'obtenir communication des données la concernant enregistrées dans le traitement sous une forme accessible et en obtenir une copie (Article 39 de la loi). »

Article 40 sur le droit de rectification :

« Toute personne peut exiger du responsable d'un traitement que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données la concernant qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite (Article 40 de la loi.) »

7.3 : Droit d'opposition :

Les citoyens ont le droit de s'opposer, pour des motifs valables, à ce que des données les concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.

L'article 38 de la loi est explicite concernant le droit d'opposition du citoyen qui saisit ce droit :

Article 38 sur le droit d'opposition

« Toute personne peut s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (Article 38 de la loi). »

e) Les données personnelles – Les sanctions :

Après avoir fait référencer les principes et les droits concernant les données personnelles, nous allons parler des obligations et des sanctions selon le contexte.

Selon la CNIL, 6 obligations doivent être respectés pour les utilisateurs de données personnelles :

- **La sécurité des fichiers :** *« Tout responsable de traitement informatique de données personnelles* ***doit adopter des mesures de sécurité physiques*** *(sécurité des locaux),* ***logiques*** *(sécurité des systèmes d'information) et* ***adaptées*** *à la nature des données et aux risques présentés par le traitement. »*

  Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende.

  Que dit le code Pénal ?

Article 226-17 :

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »

Mais que dit justement l'article 34 ?

L'article indique clairement l'obligation principale de l'acteur qui se charge du traitement des données de mettre en œuvre des obligations de moyens, des procédés aussi bien physique que logique avant de passer à l'acte.

Article 34 (extrait) :

« 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. »

- **L'information des personnes :** « *Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées. »*

  Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 € par infraction constatée et 3 000 € en cas de récidive.

Que dit le code Pénal ?

Article 131-13 (extrait) :

« Constituent des contraventions les infractions que la loi punit d'une amende n'excédant pas 3 000 euros.

Le montant de l'amende est le suivant :

1° 38 euros au plus pour les contraventions de la 1re classe ;

2° 150 euros au plus pour les contraventions de la 2e classe …. »

- **La confidentialité des données :** *« Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc). »*

  La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende.

  La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende.

  Que dit le code pénal ?

> **Article 226-22 (extrait) :**
>
> ***« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »***

- **L'autorisation de la CNIL :** Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL.

  Le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000€ d'amende.

  Que dit le code pénal ?

> **Article 226-16 (extrait) :**
>
> ***« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »***

- **La durée de conservation des informations :** Les données personnelles **ont une date de péremption**. Le responsable d'un fichier fixe **une durée de conservation raisonnable** en fonction de l'objectif du fichier.

  Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 € d'amende.

  Que dit le code pénal ?

> **Article 226-20 (extrait) :**
>
> ***« Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. »***

- **La finalité des traitements :** **Un fichier doit avoir** un objectif précis**.**

  Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif**.**

  Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité **pour laquelle elles ont été collectées.**

  Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 € d'amende.

  Que dit le code pénal ?

> **Article 226-21 (extrait) :**
>
> ***Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.***

---

2) Les données personnelles en Droit : les nouvelles lois promulguées :

Si de nombreuses lois ont été votées et appliquées ces dernières, la plus récente fait actuellement polémique puisque cette loi a été promulguée dans la cadre du programme militaire 2014-2019 :

- **Loi n° 2013-1168 du 18 décembre 2013 :** Votée en décembre 2013, cette loi est décrite en deux séries de dispositions, il y a les dispositions programmatiques (politique de défense, programmation financière), mais c'est surtout les dispositions normatives qui pose problème, c'est l'article qui le dit : «*cadre juridique du renseignement, de la cyber défense, du traitement pénal des affaires militaires, de la protection juridique accordés aux ayants droit des militaires, de mesures de gestion des ressources humaines accompagnant les réductions d'effectifs* ».

Quelles conséquences après la loi votée ?

Votée en Décembre 2013, cette loi, en rapport avec la programmation militaire entre 2014 et 2019 élargit le champ d'action des autorités dans la lutte contre la criminalité.

Concrètement, cela veut dire que les administrations peuvent donc demander l'accès direct aux informations personnelles d'un ou de plusieurs individus aux hébergeurs de sites Internet et aux fournisseurs d'accès à n'importe quel moment, et ce pour contrer la délinquance organisée et préserver le « potentiel scientifique et économique de la France. » Le tout sans passer par un juge.

Par conséquent, l'accès aux données personnelles est libre.

Que dit cette loi ?

LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

Il faut se pencher sur les articles qui traitent étroitement sur les données personnelles des citoyens français, parmi ceux validé par le conseil constitutionnel, un seul a fait débat à l'assemblé national : l'article 13

Article 13 (extrait) :

I. — L'article 154 de la loi de finances pour 2002 (n° 2001-1275 du 28 décembre 2001) est ainsi modifié :

1° Le II est ainsi rédigé :

« II. — La commission de vérification constitue une formation spécialisée de la délégation parlementaire au renseignement. Elle est composée de deux députés et de deux sénateurs, membres de la délégation parlementaire au renseignement, désignés de manière à assurer une représentation pluraliste. Le président de la commission de vérification est désigné chaque année par les membres de la délégation. » ;

II.

2° Le second alinéa du VI est ainsi rédigé :

« Le rapport est présenté aux membres de la délégation parlementaire au renseignement qui ne sont pas membres de la commission. Il est également remis, par le président de la délégation, aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances ainsi qu'au Président de la République et au Premier ministre…. »

Ce désormais célèbre article 13 introduit dans le code de la défense un nouveau chapitre VI intitulé « *Accès administratif aux données de connexion* ». Dans ce chapitre VI, un nouvel article L 246-1 autorise les ministères de la défense, de l'intérieur et de l'économie et des finances à accéder aux « *informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques* », c'est à dire aux identifiants de connexion, à la localisation des équipements utilisés.

Voici le contenu exact du chapitre IV, à l'article 246-1 :

« *Art. L. 246-1.* – Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique…. »

Enfin, l'effet de l'article du code de la défense prendra effet dès 2015, d'où le contenu de l'article suivant :

« IV. – Le présent article entre en vigueur le 1er janvier 2015. »

Conclusion :

Nous constatons qu'il y a des principes, des règles, des droits et des devoirs concernant tout le monde qui ont étaient établie par la loi « Informatique et Libertés » et qui permettent d'encadrer la façon dont les données personnelles doivent être traitées. Aujourd'hui, plus que jamais, la CNIL devient un acteur incontournable, malgré les limites à faire respecter les lois face aux géants d'Internet (Google, Facebook, Apple et Amazon notamment) qui ont plus de pouvoirs que les gouvernements européens.

Plus ça va et pire c'est, la surveillance d'Internet se renforce de plus en plus, malgré les scandales des écoutes de la NSA révélé par l'ancien consultant Edward Snowden, ça aurait pu permettre à l'Europe d'affirmer sa volonté de créer un réseau européen, c'est exactement ce que veut la chancelière allemande Angela Merkel, où elle souhaite créer un câble qui passe non part depuis les Etats-Unis, mais depuis le Brésil, hélas, Paris reste réservé à ce sujet, bien qu'une conférence mondiale aura lieu en 2015 en faveur de « la gouvernance d'Internet ».

En France, la loi sur la programmation militaire qui s'étalera de 2014 à 2015 a été votée sans colère ni contestation de la part des citoyens français, en effet, malgré des débats autour du fameux article 13 qui est effectivement un danger pour les données personnelles des citoyens et qui aurait dû être jugé anticonstitutionnel, ce qui n'était pas le cas. Et c'est le paradoxe, on a plus qu'à s'attendre aux pires car dès l'an prochain, il faudra nous citoyens se donner les moyens pour rendre les tâches aux agents de renseignements plus durs de consulter nos données personnelles.