La loi pour une République numérique protège encore plus nos données personnelles

	La loi pour une République numérique protège encore plus nos données personnelles

Quels sont les apports de la loi république numérique en matière de protection des données personnelles ?

La loi pour une République numérique du 7 octobre 2016 crée de nouveaux droits informatique et libertés et permet ainsi aux individus de mieux maîtriser leurs données personnelles. Elle renforce les pouvoirs de sanctions de la CNIL et lui confie de nouvelles missions. Elle contribue également à une meilleure ouverture des données publiques.
Certaines dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018.
Publiée au Journal Officiel du 8 octobre 2016, la loi pour une république numérique introduit de nombreuses dispositions directement applicables, d'autres doivent attendre la publication de décrets d'application. Nous recensons ci-dessous les dispositions d'application directe. Ce recensement sera mis à jour au fur et à mesure de la publication des décrets d'application.

De nouveaux droits pour les personnes

L'affirmation du principe de la maîtrise par l'individu de ses données
Le droit à l'autodétermination informationnelle s'inspire d'un droit similaire dégagé par la juridiction constitutionnelle allemande. Il renforce positivement les principes énoncés à l'article 1er de la loi Informatique et Libertés en affirmant la nécessaire maîtrise de l'individu sur ses données.

Le droit à l'oubli pour les mineurs
L'article 40 de la loi Informatique et libertés prévoit désormais un « droit à l'oubli » spécifique aux mineurs et **une procédure accélérée pour l'exercice de ce droit**. Lorsque la personne concernée était mineure au moment de la collecte des données, elle peut obtenir auprès des plateformes l'effacement des données problématiques « dans les meilleurs délais ».
En l'absence de réponse ou de réponse négative de la plateforme dans un délai de un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de 3 semaines pour y répondre.

La possibilité d'organiser le sort de ses données personnelles après la mort
Le nouvel article 40-1 de la loi Informatique et libertés permet aux personnes de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.
Une personne peut être désignée pour exécuter ces directives. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés.
Ces directives sont :
• générales, lorsqu'elles portent sur l'ensemble des données concernant une personne ;
• ou particulières, lorsque ces directives ne concernent que certains traitements de données spécifiques.

Lorsque ces directives sont générales et portent sur l'ensemble des données du défunt, elles peuvent être confiées à un tiers de confiance certifié par la CNIL.

Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement (réseaux sociaux, messagerie en ligne) en cas de décès. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
En l'absence de directives données de son vivant par la personne, les héritiers auront la possibilité d'exercer certains droits, en particulier :
1. le droit d'accès, s'il est nécessaire pour le règlement de la succession du défunt ;
2. le droit d'opposition pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer au traitement de leurs données.

La possibilité d'exercer ses droits par voie électronique
Le nouvel article 43 bis de la loi Informatique et Libertés impose, « lorsque cela est possible », de permettre à toute personne l'exercice des droits d'accès, de rectification ou d'opposition par voie électronique, si le responsable du traitement des données les a collectées par ce vecteur.

Plus d'information et de transparence sur le traitement des données.

L'information des personnes sur la durée de conservation de leurs données
L'obligation d'information prévue par l'article 32 de la loi Informatique et Libertés est renforcée. Les responsables de traitements de données doivent désormais informer les personnes de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Les compétences de la CNIL confortées et élargies

Un pouvoir de sanction renforcé
Le plafond maximal des sanctions de la CNIL **passe de 150.000€ à 3 millions €** (anticipation sur l'augmentation du plafond du montant des sanctions par le règlement européen qui sera applicable le 25 mai 2018 et prévoit un plafond pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial).
La formation restreinte de la CNIL peut désormais ordonner que les organismes sanctionnés informent individuellement de cette sanction et à leur frais, chacune des personnes concernées.
Elle pourra également prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité.

Une consultation plus systématique de la CNIL.
La CNIL sera saisie pour avis sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Cette rédaction permettra à la CNIL d'apporter son expertise aux pouvoirs publics de manière plus systématique, alors que les textes actuels ne prévoient sa saisine que sur les dispositions relatives à la « protection » des données personnelles.

La publicité automatique des avis de la CNIL sur les projets de loi.
Cette disposition renforce la transparence sur les avis de la CNIL.

De nouvelles missions :
• **L'affirmation de sa mission de promotion de l'utilisation des technologies protectrices de la vie privée**, notamment les technologies de chiffrement des données.
• **La certification de la conformité des processus d'anonymisation** des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation. L'anonymisation des bases de données est une condition essentielle à leur ouverture ou à leur partage : elle permet de prémunir les personnes des risques de ré-identification, et les acteurs (administrations émettrices de données, ré-utilisateurs, entreprises privées qui réalisent des recherches notamment statistiques), de la mise en cause de leur responsabilité en la matière. La certification ou l'homologation de méthodologies d'anonymisation ainsi que la publication de référentiels ou de méthodologies générales par la CNIL sera ainsi un gage de protection des personnes et de sécurité juridique pour les acteurs.
• **La conduite par la CNIL d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.** Même si la loi Informatique et Libertés a toujours comporté une dimension éthique fondamentale, comme en témoignent tant ses conditions de création et son article 1er, que la composition de la Commission, la révolution numérique implique une réflexion élargie sur sa dimension éthique.

L'ouverture des données publiques étendue

La loi pour une république numérique ne remet pas en cause l'équilibre entre transparence administrative et protection de la vie privée et des données personnelles. En effet, les critères de communicabilité n'ont pas changé, et la publication – donc la réutilisation – est subordonnée au caractère librement communicable du document.
Pour autant, en passant d'une logique de la demande d'un accès à une logique de l'offre de données publiques, la loi vise clairement à ouvrir très largement les données publiques. La CNIL va accompagner cette ouverture, notamment en répondant aux demandes de conseil des collectivités publiques ou des réutilisateurs, puisque toute réutilisation de données personnelles est soumise au « droit commun » Informatique et Libertés. La possibilité pour la CNIL d'homologuer des méthodologies d'anonymisation constituera un élément important de cette régulation.
En matière de gouvernance de la donnée, la loi prévoit un rapprochement entre la CNIL et la CADA, à travers, notamment, une participation croisée dans les deux collèges.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ce que change la loi pour une République numérique pour la protection des données personnelles | CNIL

Que prévoit la loi pour les Hackers éthiques ?

Que prévoit la loi pour les Hackers éthiques ?

La loi pour une République numérique protège les hackers éthiques et confirme le rôle central de l'Anssi dans le signalement de failles informatiques. Les explications de l'avocat François Coupez.

En complétant le code de la défense, la loi du 7 octobre 2016 pour une République numérique entérine la protection des hackers éthiques. En tout cas ceux qui signalent une faille informatique découverte par leurs soins à l'Agence nationale pour la sécurité des systèmes d'information (Anssi). La législation confirme ainsi le rôle central de cette dernière dans le signalement des vulnérabilités.
« Ce texte va surtout permettre une officialisation », explique à *Silicon.fr* François Coupez, avocat associé du cabinet Atipic. *« L'Anssi apparaît bien comme le second point de contact officiel, en plus du responsable du système d'information objet des vulnérabilités »*. Ce point de contact *« est utile pour les cas où les 'hackers éthiques' supposeraient qu'ils ne peuvent joindre directement l'entité dont le SI est vulnérable, quelle qu'en soit la raison : responsable supposé peu réceptif, responsable déjà contacté en vain, etc. »*.

Protéger le hacker dit « éthique »

Pour distinguer le hacker éthique du pirate (l'article 323-1 du code pénal sanctionne le piratage frauduleux d'au moins deux ans d'emprisonnement et de 60 000 euros d'amende), l'article 47 de la loi numérique complète le code de la défense par un article L2321-4 ainsi rédigé :
« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.
L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.
L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Sécuriser les agents de l'Anssi

Rappelons que l'article 40 du code pénal cité dans cet article L2321-4 indique : *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »*
Or, dans la loi portée par Axelle Lemaire, cette obligation prévue à l'article 40 ne s'applique pas aux *white hats*. Ce qui arrivait déjà, en fait, avant la promulgation du texte. *« D'après ce qu'a pu indiquer à certaines occasions l'Anssi elle-même, la pratique interne était déjà de ne pas appliquer l'article 40 dans les hypothèses similaires à celles visées par cet article L2321-4 du code de la défense nouvellement créé. Et ce afin de faciliter les remontées d'informations. Ce que la loi République numérique légitime dorénavant via cet article, et c'est une très bonne chose pour la sécurité juridique des agents de l'Anssi »*, ajoute François Coupez…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Hacker éthique : la législation française enfin claire ?

Le projet de loi République Numérique enfin adopté

Le projet de loi République Numérique enfin adopté

Après avoir été adopté par l'Assemblée Nationale au mois de juillet dernier, le projet de loi République Numérique l'a été à son tour par le Sénat. Sauf saisine du Conseil Constitutionnel dans les 15 prochains jours, la loi devrait donc être promulguée rapidement et plusieurs choses devraient donc changer dans les semaines à venir.

L'open data, une des nouveautés du projet de loi République Numérique

A l'occasion de sa séance publique du 28 septembre 2016, le Sénat a adopté définitivement le projet de loi « République Numérique » et ce à l'unanimité.
Deux mois après, les sénateurs font donc le même choix que les députés ce qui signifie que la promulgation de ce texte est pour bientôt.
Parmi les nouveautés qu'il apporte, il y a l'open data. En effet, ce projet de loi prévoit l'ouverture d'une partie des données de l'administration publique mais aussi des données de certaines sociétés du secteur privé ayant une mission de service public. Ceci est en particulier une grande avancée pour la recherche puisque des données à l'accès restreint seront accessibles à un public plus large.

Vers un meilleur accès aux réseaux numériques

Initié par Axelle Lemaire, secrétaire d'Etat chargée du Numérique, le projet de loi République Numérique a vocation à faciliter l'entrée de la République dans l'ère du numérique.
Par conséquent, les idées et mesures présentes dans le texte sont nombreuses et variées et visent à :

- Améliorer la protection des données sur le web
- Rendre accessible Internet au plus grand nombre
- Mettre en concurrence tous les acteurs de l'Internet
- Rendre obligatoire l'information « claire et loyale » des clients
- Accélérer la couverture du territoire en très haut débit
- Rendre accessible les contenus numériques aux personnes souffrant de handicap (visuel, auditif, etc…)
- Reconnaître le e-sport et définir le statut des joueurs

Autrement dit, la loi République Numérique devrait éclaircir bien des situations et cas complexes…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le projet de loi République Numérique enfin adopté

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

	Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Le nouveau règlement européen relatif à la protection des données personnelles (GDPR) fait grand bruit en Europe. Il donne, en effet, plus de droits aux consommateurs sur la façon dont leurs données sont traitées et requiert des contrôles complémentaires (et des informations) sur quiconque dispose de données personnelles dans l'Union européenne.

Comme toutes les lois, celle-ci a été largement discutée, avec des points de vue contradictoires, mais une chose a été acceptée par tous : les entreprises auront deux ans, à compter de la date de publication de la loi (en juin 2016), avant que celle-ci entre en vigueur. Deux années indispensables aux entreprises pour leur permettre de mettre en place les politiques, les processus et les technologies nécessaires pour être en conformité avec le règlement.
En avance sur ses voisins européens, la France a d'ores et déjà adopté un projet de loi en phase avec les principes fondamentaux du règlement européen relatif à la protection des données personnelles. Ainsi, le projet de loi pour une République numérique, validé par l'Assemblée nationale le 26 janvier dernier (actuellement examiné par le Sénat), devrait être approuvé pour entrer en vigueur cette année.

Quelles sont les grandes lignes de la loi pour la République numérique ?

Droit à la portabilité des données : le consommateur peut demander à ce que ses données soient conservées par le responsable du traitement des données et dispose en toutes circonstances d'un droit de récupération de ses données.
• Conservation des données : le responsable du traitement des données doit informer le consommateur de la durée pendant laquelle les données sont conservées.
• Droit de rectification : les consommateurs peuvent demander à ce que leurs données soient éditées pour les modifier.
• Droit à la suppression : les personnes concernées peuvent demander à ce que leurs données soient supprimées ou interdire l'usage de leurs données.
• Recours collectifs : les consommateurs peuvent déposer une plainte collective pour demander réparation lors de la perte ou de l'utilisation abusive de leurs données.
• Amende maximale : celle-ci peut aller de 150.000 à 20.000.000 euros ou 4 % du chiffre d'affaires global, pour l'amende la plus élevée.
D'autres pays vont-ils prendre exemple sur la France pour faire avancer leurs propres législations sur la protection des données avant la mise en œuvre du règlement européen ? Il y a fort à parier que oui. Et les entreprises ont également anticipé cette nouvelle réglementation puisque l'utilisation de services cloud basés dans la zone européenne a presque doublé en six mois (de 14,3 % au premier trimestre 2015 à 27 % pour 2016)… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur les données personnelles : la France en avance sur ses voisins européens – Global Security Mag Online*

Ce que va changer la Loi sur le numérique à propos de la protection des données personnelles | Le Net Expert Informatique

	**Ce que va changer la Loi sur le numérique à propos de la protection des données personnelles**

Secret des correspondances, droit à l'oubli ou encore pouvoirs de la Cnil… Le projet de loi veut imposer le concept de libre disposition des données personnelles d'un utilisateur.

Le tant attendu projet de loi pour la République numérique d'Axelle Lemaire a enfin pris forme. Fruit d'une grande concertation nationale de près d'un an, le projet de loi est désormais soumis à une ultime consultation en ligne jusqu'au 18 octobre. L'occasion pour le JDN de faire le point sur les différents volets de ce projet de loi participatif.

Cette loi est « une loi de progrès du droit », explique le gouvernement. Une loi qui affirme les grands principes nécessaires à la protection des citoyens, en matière de données personnelles notamment, nous promet-on. Ainsi le projet de loi prend-t-il le soin de réaffirmer le fameux secret des correspondances dans un article 22 qui stipule que « tout traitement automatisé d'analyse du contenu de la correspondance en ligne ou des documents joints a`celle-ci constitue une atteinte au secret des correspondances, sauf lorsque ce traitement a pour fonction l'affichage, le tri ou l'acheminement de ces correspondances, ou la détection de contenus non sollicités ou malveillants ». Oui, Gmail, Outlook ou Yahoo mail peuvent étudier vos échanges d'emails s'il s'agit de mettre en exergue ceux-qui sont les plus à même de vous intéresser ou, au contraire, de filtrer les spams.

Google ne pourra plus lire vos mails pour des pubs ciblées

« Ces services ne pourront en revanche plus examiner automatiquement le contenu des correspondances privées échangées en leur sein pour des fins commerciales, comme ils pouvaient le faire jusque-là », explique Alan Walter, avocat associé au sein du cabinet Walter Billet. La fin de la publicité ciblée via le scan des mails dans Gmail et consorts ? Les Français pourront en tout cas désormais invoquer l'article 226.1 et suivant du code Pénal pour poursuivre en justice les contrevenants. Mais l'histoire récente montre qu'un tel combat judiciaire ne peut se mener avec succès que s'il est mené à l'échelle européenne. Ne reste plus qu'à espérer qu'il fera effet domino chez nos voisins.

Alors que la quantité des données nous concernant, online, croît de manière exponentielle, la loi veut redonner le contrôle aux individus sur leurs données personnelles. C'est le principe de la « libre disposition de ses données » de l'article 16 qui se veut une alternative à l'absence d'un droit de propriété sur les données. Et dans cette perspective, le projet de loi fait de la Cnil un véritable garde-fou entre l'internaute et les services de traitement de données. Sur le droit à l'oubli des mineurs, celle-ci pourra être saisie en cas d'absence ou d'absence de réponse de la part du responsable de traitement. Elle se prononcera sur la demande dans « un délai de 15 jours », affirme le projet de loi. Un vœu pieux selon Alan Walter qui affirme que « l'institution va vite être dépassée ». Une prédiction que les problèmes rencontrés par Google au moment d'appliquer lui-même le droit à l'oubli (56 jours pour traiter les demandes au début) semble conforter.

Plus de prérogatives pour la Cnil… Mais quid des moyens ?

L'avocat estime qu'il en va de même pour l'article 17 qui propose au président d'assemblée parlementaire de « soumettre a`l'avis de la commission une proposition de loi comportant des dispositions relatives a`la protection des données a`caractère personnel » et l'article 18 qui donne à la Cnil le pouvoir de « certifier la conformité du processus d'anonymisation totale ou partielles de jeux de données à caractère personnel ». « C'est très positif de donner plus de prérogatives à l'institution mais, s'il y a une nette amélioration récemment, on se rend compte que les gens de la Cnil n'ont eux-mêmes pas toujours le temps de répondre à nos sollicitations », explique-t-il. « Et je doute qu'ils soient vraiment outillés pour le faire à un tel rythme et une telle échelle avant quelques années ». D'autant que se profile dans les années à venir une fusion compliquées avec la Cada.

L'article 21 du projet de loi renforce en tout cas la procédure de sanction de la Cnil, qui pourra prononcer « une sanction immédiate lorsque le manquement ne peut pas être réparé. Dans un exercice de pédagogie, le gouvernement donne l'exemple suivant : « la CNIL pourra sanctionner financièrement une entreprise ayant perdu des milliers d'adresses email, ce qui n'est pas possible aujourd'hui (simple mise en demeure) ». Le projet de loi propose également de raccourcir les délais de mise en demeure en cas d'urgence, le ramenant à 24 heures. « On notera quand même que le montant de la sanction pécuniaire ne bouge lui pas », note Alan Walter, un brin taquin. D'un montant maximal de 150 000 euros, et, en cas de récidive, jusqu'à 300 000 euros. Un montant par vraiment dissuassif pour les géants américains.

Source : http://www.journaldunet.com/ebusiness/le-net/1164005-protection-des-donnees-personnelles-loi-sur-le-numerique/

Par Nicolas Jaimes — JDN