# BULLETIN D'ACTUALITES JURIDIQUES

## N°39, 15 avril 2015

### La CNIL passe au crible les systèmes d'exploitation Android

*CNIL, Lettre IP n°8, « Mobilitics, saison 2 : Les smartphones et leurs apps sous le microscope de la CNIL et l'Inria », nov. 2014*

En 2011, la CNIL et l'Inria ont débuté une étude portant sur l'écosystème des *smartphones*. A cette occasion, un outil de détection des accès aux données personnelles stockées dans les appareils a été développé. Une première vague de tests s'est déroulée début 2013 sur les équipements Apple. Les résultats en ont été publiés en avril de la même année.

Le 15 décembre 2014, la Commission a rendu publics les résultats d'une nouvelle étude, portant cette fois, sur les appareils équipés d'Android. Ces résultats concordent avec les constats obtenus précédemment. La CNIL a observé que près de 60% des applications testées accédaient aux identifiants du téléphone, tandis qu'un tiers accédaient aux données de localisation. En volume, les données de géolocalisation sont apparues comme étant les plus collectées, notamment par les applications de jeu. Enfin, la CNIL a regretté que certains services soient installés par défaut, parfois sans qu'il soit possible de les désinstaller, alors même qu'ils collectent massivement les données générées par le *smartphone*.

Dès lors, la Commission incite les éditeurs et développeurs d'applications à adopter une approche dite de « *privacy by design* » et à ne collecter que les données strictement nécessaires à la délivrance du service rendu par l'application. Dans ce cadre, elle invite les acteurs du marché à se référer à l'avis sur les applications destinées aux dispositifs intelligents publié par le G29 en 2013.

### Nouvelle norme simplifiée de la CNIL sur les écoutes téléphoniques professionnelles

*Délibération n°2014-474 du 27 nov. 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics et privés destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail (NS 057)*

Le 27 novembre 2014, la CNIL a adopté la norme simplifiée n°57, relative aux traitements automatisés de données à caractère personnel, mis en œuvre par les organismes publics et privés, et destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail. Cette délibération concerne les enregistrements ponctuels à des fins de formation et d'évaluation des salariés, ainsi que d'amélioration de la qualité du service. Il couvre également les documents d'analyse des enregistrements, tels que les grilles d'évaluation.

Cette norme simplifiée était attendue dans de nombreuses professions, car elle va désormais faciliter les formalités de déclaration à la CNIL des traitements qui y sont conformes.

### Nouveau label CNIL : « Gouvernance informatique et libertés »

*Délibération n°2014-500 du 11 déc. 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés*

Par une délibération du 11 décembre 2014, la CNIL a adopté le référentiel d'un 4e label, consacré aux procédures de « Gouvernance informatique et libertés ». Celui-ci définit les règles et les bonnes pratiques en vue d'assurer une gestion des données respectueuse des principes « informatique et libertés ». Tout organisme justifiant auprès de la CNIL de sa conformité aux 25 exigences énoncées par le texte peut aujourd'hui obtenir ce label, vecteur de confiance et, très certainement, atout en termes d'image. La mise en conformité avec le référentiel permet aux organismes de s'inscrire dès maintenant dans une démarche d'« *accountability* », qui devrait s'imposer lorsque le projet de règlement européen sur les données personnelles sera adopté. Preuve de l'intérêt pour ce dispositif, la

CNIL a déjà reçu un grand nombre de demandes de labellisation.

Pour être labellisé, l'organisme doit, notamment, faire la preuve qu'il dispose d'une politique de protection des données personnelles, avoir procédé à une désignation étendue d'un correspondant informatique et libertés et avoir mis en place un processus de gestion des données personnelles. Cette dernière exigence suppose souvent une expertise spécifique dans le domaine.

## Internet Wi-Fi en libre accès : la CNIL dresse un bilan

*CNIL, « Internet et wi-fi en libre accès : bilan des contrôles de la CNIL », 22 déc. 2014*

Dans le cadre de son programme des contrôles 2014, la CNIL s'est intéressée à la mise à disposition d'un accès à Internet au public. Dans son bilan, elle a constaté que la plupart des services concernés ne satisfaisaient pas aux exigences de la loi « informatique et libertés ».

La Commission a commencé par rappeler que les organismes concernés sont soumis aux exigences de l'article L.34-1 du Code des postes et des communications électroniques (CPCE), qui prohibe notamment la conservation des données de contenu et encadre strictement la conservation des données relatives au trafic. Par ailleurs, le respect de ces dispositions ne dispense pas l'organisme, en tant que responsable de traitement, de respecter les exigences de la loi « informatique et libertés », et en particulier d'informer les personnes concernées.

## Projet de loi numérique : propositions d'évolutions de la loi « informatique et libertés »

*Propositions de la CNIL sur les évolutions de la loi informatique et libertés dans le cadre du projet de loi numérique, 13 janv.2015*

En 2013, le gouvernement a annoncé travailler sur un projet de loi numérique, destiné à être soumis au Parlement courant 2015, et faisant notamment évoluer la loi « informatique et libertés ». Dans ce cadre, la CNIL vient de publier plusieurs propositions.

La Commission suggère notamment de renforcer l'effectivité des droits des personnes concernées. A ce titre, elle souhaite introduire explicitement, dans les dispositions légales, la possibilité d'exercice des droits d'opposition, d'accès et de rectification par voie électronique. Elle propose également de permettre à toute personne d'obtenir l'effacement des données la concernant relatives à la période où elle était mineure, sans avoir à justifier d'un quelconque motif. La CNIL souhaite ensuite la simplification des formalités relatives aux transferts de données personnelles hors de l'Union européenne pour les entreprises disposant de « BCR » (*Binding Corporate Rules*), c'est à dire de règles internes. A cette fin, elle envisage de délivrer une autorisation unique à chaque groupe en ayant adopté. Elle propose, par ailleurs, de reconnaître une coresponsabilité sur les traitements, qui permettrait de mieux refléter la réalité de certaines relations entre le responsable de traitement et ses sous-traitants. Enfin, en cohérence avec le projet de règlement européen pour la protection des données, la CNIL demande une augmentation du maximum des sanctions pécuniaires qu'elle peut prononcer, en proposant que ce montant soit exprimé en pourcentage du chiffre d'affaires de l'organisme condamné.

## Révision des formulaires de déclaration et d'autorisation en matière de cryptologie

*Arrêté du 29 janv. 2015 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie*

Si la LCEN (loi pour la confiance dans l'économie numérique du 21 juin 2004) a libéralisé l'utilisation des moyens de cryptologie, la fourniture, l'importation et l'exportation des outils de chiffrement visant à assurer la confidentialité des données demeurent soumis au principe de déclaration ou de demande d'autorisation préalable au Premier ministre. L'arrêté du 29 janvier 2015 est venu réviser les formulaires de déclaration et de demande d'autorisation à adresser à l'ANSSI dans le cadre de cette procédure. Les trois formulaires sont désormais regroupés au sein d'un unique document, dans un souci de simplification.

## L'ANSSI fixe des mesures de sécurité pour les systèmes d'information sensibles

*Instruction ministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI*

Le 28 janvier 2015, l'ANSSI a produit une nouvelle instruction interministérielle relative à la protection des systèmes d'information sensibles. Celle-ci remplace les instructions de 1993 et 1994, consacrées à la protection des informations sensibles non classifiées et à la protection des systèmes d'information traitant de ce type d'informations.

Cette instruction s'impose aux administrations de l'Etat et aux entités, publiques ou privées, soumises aux exigences relatives à la protection du potentiel scientifique et technique de la Nation qui mettent en œuvre des systèmes d'information sensibles, ainsi qu'à toute autre entité disposant de systèmes d'information « diffusion restreinte ». Elle a également vocation à guider tout organisme mettant en œuvre des systèmes d'information sensibles.

Des processus et mesures de sécurité sont énoncés aux titres II et III, ainsi qu'en annexe 1. Les entités mettant en œuvre des systèmes d'information sensibles doivent appliquer les mesures énoncées au titre II. Les administrations de l'Etat mettant en œuvre la PSSIE (circulaire du Premier ministre du 17 juillet 2014, BAJ n°35 du 21 octobre 2014) sont présumées conformes à ces exigences. En revanche, les entités qui ne sont pas soumises à la PSSIE doivent mettre en œuvre les mesures détaillées à l'annexe 1 de l'instruction. Le titre III énonce quant à lui des mesures supplémentaires applicables aux systèmes d'information « diffusion restreinte ».

Les organismes ayant déjà mis en place un système d'information « diffusion restreinte » au jour de la publication de l'instruction disposent de 3 ans pour se conformer à ces exigences. Pour les autres, le délai est de 6 mois.

## Mise en œuvre du blocage administratif d'accès aux sites illicites

*Décret n°2015-125 du 5 fév. 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et de sites diffusant des images et représentations de mineurs à caractère pornographique*

Le décret d'application de la loi du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme, est entré en vigueur le 7 février 2015. Ainsi, à compter de cette date, le cadre légal et réglementaire relatif au blocage administratif des contenus provoquant à des actes de terrorisme et des contenus à caractère pédopornographiques est applicable.

La procédure de blocage administratif de ces sites est la suivante : lorsque les agents dûment habilités de l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) constatent la mise en ligne de contenus illicites, ils adressent à l'éditeur une demande de retrait. Simultanément, ils informent les fournisseurs d'accès à Internet (FAI). En l'absence de retrait de ces contenus par l'éditeur dans les 24 heures, les agents notifient aux FAI la liste des sites illicites. Les fournisseurs d'accès doivent alors empêcher, dans les 24 heures suivant la notification, l'accès à ces sites par tout moyen approprié. Les agents de l'OCLCTIC peuvent également notifier la liste des sites aux moteurs de recherche ou aux annuaires. Ces derniers doivent alors prendre toute mesure utile pour faire cesser le référencement des contenus. Quant aux internautes tentant de consulter les pages ainsi bloquées, ils sont redirigés vers une mention d'information du ministère de l'intérieur, indiquant la raison du blocage et les voies de recours.

Dans le même temps, les agents de l'OCLCTIC doivent transmettre leurs demandes de blocage à une personnalité qualifiée au sein de la CNIL. Celle-ci s'assure alors de la régularité de la procédure. Si elle constate un problème, elle recommande à l'autorité administrative d'y mettre fin. Dans l'hypothèse où sa recommandation ne serait pas suivie, la personnalité qualifiée pourrait saisir la juridiction compétente. Un rapport d'activité consacré aux demandes de retrait sera publié chaque année.

En décembre 2014, la CNIL avait donné son avis sur le projet de décret. Elle avait rappelé que la Cour de justice de l'Union européenne avait invalidé la directive dite « *Data Retention* » (arrêt *Digital Rights*

du 8 avril 2014 ; BAJ n°30 du 22 avril 2014). Dès lors, les dispositions de la loi de programmation militaire relatives au blocage administratif d'accès et de ses décrets d'application pouvaient s'avérer inconventionnelles, c'est-à-dire non-conformes aux traités de l'Union. La Quadrature du net a d'ailleurs saisi le Conseil d'Etat, le 18 février 2015, afin qu'il se prononce sur ce point.

## Les SMS des téléphones portables d'entreprise sont présumés professionnels

*Cass. com., 10 fév. 2015, n°13-14.779, sté Newedge Group c. sté GFI Securities Ltd.*

La société Newedge Group, qui reprochait à sa concurrente GFI d'avoir débauché un grand nombre de ses salariés, et d'avoir ainsi provoqué la désorganisation de son activité, a été autorisée, par ordonnance sur requête, à procéder à constat d'huissier portant sur les outils de communication qu'elle avait mis à la disposition de ses anciens salariés. L'objectif du constat était de consulter le contenu les SMS envoyés et reçus sur les téléphones mobiles professionnels. La société GFI a demandé la rétractation de l'ordonnance, mais, le juge des référés, puis la Cour d'appel, ont rejeté sa demande.

Par un arrêt du 10 février 2015, la chambre commerciale de la Cour de cassation a précisé que « les messages écrits […] envoyés ou reçus par le salarié au moyen du téléphone mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ». Ainsi, la Cour estime que la production en justice des SMS n'ayant pas été identifiés comme personnels par le salarié est possible, car la preuve n'a pas été recueillie par un procédé déloyal.

Cette décision s'inscrit dans une jurisprudence constante. Elle étend simplement aux SMS la solution déjà adoptée pour les fichiers stockés sur le matériel professionnel (Cass. soc., 18 oct. 2006, M. X. c/ Sté Techni-Soft) et les courriels émis et reçus sur la messagerie mise à la disposition des salariés par leur employeur (Cass. soc., 18 oct. 2011, M. X. c/ Sté Nova).

**L'équipe juridique HSC**

juridique@hsc.fr , 01 41 40 97 00

| Les prochaines formations juridiques HSC - 2015 | | | |
|---|---|---|---|
| **Formations principalement juridiques** | | | |
| **Correspondant informatique et libertés** | Lyon, 5-7 mai | Rennes, 8-10 juin | Strasbourg, 22-24 juin |
| **Essentiels juridiques pour gérer la SSI** | Paris, 21-22 mai | Paris, 26-27 novembre | |
| **Essentiels Informatiques et libertés** | Paris, 18 mai | Paris, 13 novembre | |
| **Formations comportant une partie juridique** | | | |
| **PKI** | Paris, 4-6 mai | | |
| **RGS v.2** | Paris, 29 mai | Paris, 6 novembre | |
| **RSSI** | Paris, 30 mars – 3 avril | Paris, 5-9 octobre | |
| **Sécurité du *cloud computing*** | Paris, 26-28 mai | Paris, 21-23 octobre | |
| **Tests d'intrusion avancés, exploits, hacking éthique (SANS SEC560)**** | Paris, 16-20 mars | Paris, 19-23 octobre | |

** : Formation certifiante

**formations@hsc.fr, 01 41 40 97 00**

Ce bulletin d'actualités juridiques est édité par la société Hervé Schauer Consultants, SASU au capital de 300 000 euros, inscrite au RCS Nanterre B 444 475 891, sise 191, avenue Charles-de-Gaulle, 92 200 NEUILLY-SUR-SEINE. Son directeur de publication est Hervé Schauer, Directeur général.
Contact : juridique@hsc.fr ou 01 41 40 97 00.