

BULLETIN D'ACTUALITES JURIDIQUES

N°40, 29 mai 2015

Projet de loi relatif au renseignement : mise en place de la surveillance internationale

CNIL, Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement

Projet de loi relatif au renseignement adopté par l'Assemblée nationale et enregistré par le Président du Sénat le 5 mai 2015

Le 5 mars 2015, la CNIL a donné son avis sur le projet de loi relatif au renseignement. Si certaines de ses remarques ont été prises en compte depuis le dépôt du projet de loi, d'autres n'ont encore été reprises par aucun amendement. Les dispositions consacrées à la surveillance internationale, notamment, n'ont été que peu retouchées. Or, la CNIL a regretté que les mesures de surveillance et les données collectées dans le cadre de ces opérations ne soient pas définies. Certes, un décret en Conseil d'Etat précisera, « en tant que besoin », les modalités de mise en œuvre des opérations et du contrôle des communications, mais les dérives possibles demeurent nombreuses. Ainsi, la surveillance internationale sera soumise à une procédure d'autorisation spécifique, sans avis préalable de la future Commission nationale de contrôle des techniques de renseignement (CNCTR). Celle-ci ne réalisera qu'un contrôle *a posteriori*, donnant lieu, au moins chaque semestre, à la rédaction d'un rapport soumis au Premier ministre. Ce dernier devra répondre par une décision motivée aux éventuelles recommandations et observations présentées dans ce rapport. Il reste maintenant à savoir si le projet actuellement discuté restera en l'état sur ces questions, ou s'il évoluera, d'ici son adoption définitive, dans le sens d'un renforcement des garanties liées à la surveillance.

BCR et transferts internationaux de données : la CNIL délivre des autorisations uniques

CNIL, « BCR : la CNIL facilite les formalités liées aux transferts internationaux de données », Actualité, 24 mars 2015

Jusqu'alors, l'adoption de règles internes d'entreprise au sein d'un groupe international ne dispensait pas le responsable de traitement de la demande d'autorisation préalable aux transferts de données extracommunautaires entre les entités de ce groupe.

Le 24 mars 2015, la CNIL a annoncé qu'elle délivrera désormais une autorisation unique à chaque groupe ayant adopté des BCR (*Binding Corporate Rules*). Cette autorisation dispensera le groupe de procéder à une demande d'autorisation pour chaque type de transfert en dehors de l'Union européenne envisagé. Le contenu de ces autorisations uniques sera défini par la Commission, en collaboration avec chacun des groupes. A cette fin, la CNIL contactera les organismes ayant déjà des BCR dans les prochains mois. Grâce à ces autorisations uniques, les entités du groupe auront simplement à déposer un engagement de conformité sur le site de la CNIL. Le groupe, quant à lui, devra tenir une liste des transferts réalisés.

Déchiffrement des flux https : la CNIL délivre son analyse

CNIL, « Analyse de flux https : bonnes pratiques et questions », Actualité, 31 mars 2015

De plus en plus d'entreprises souhaitent procéder au déchiffrement puis au rechiffrement des flux https sortants, afin de pouvoir les surveiller. Se pose alors la question de la légalité de cette pratique. L'ANSSI avait déjà traité de ce sujet l'année dernière, et avait conclu à la licéité du procédé, en allant même jusqu'à l'encourager (voir BAJ n°36 du 20 novembre 2014). En mars dernier, c'est la CNIL qui s'est prononcée sur la conformité de ce nouvel usage à la loi « informatique et libertés ».

Dans sa note d'actualité du 31 mars 2015, la Commission a estimé qu'un tel déchiffrement était légitime, l'employeur ayant l'obligation d'assurer la sécurité de son système d'information. Pour autant, les opérations réalisées doivent respecter les exigences érigées par la loi « informatique et libertés ». Ainsi, seules les données strictement nécessaires pour assurer la sécurité du système d'information doivent être collectées, elles doivent être traitées de façon sécurisée et leur durée de conservation doit être limitée. Enfin,

la CNIL a rappelé que ce procédé devait faire l'objet d'une information précise des salariés, notamment par le biais de la charte informatique de l'organisme (pour aller plus loin, voir « La charte informatique face aux nouveaux usages de l'entreprise », GS-Days, 18 mars 2014).

Publication du rapport annuel d'activité 2014 de la CNIL

CNIL, Rapport annuel d'activité 2014, 35^e rapport, 15 avril 2015

Le 15 avril 2015, la CNIL a publié son 35^e rapport d'activité, portant sur l'année 2014. Il en ressort que l'année passée a été celle de la conformité, des contrôles et de la protection des personnes concernées.

La conformité, d'abord, a été un véritable sujet pour la CNIL, avec le développement des outils de régulation. Les « packs » se sont multipliés, afin d'accompagner les professionnels dans leur démarche de mise en conformité « informatique et libertés ». De plus, trois nouveaux labels ont été créés : un pour les services de coffre-fort numérique, un autre pour les prestations d'audit de traitement, et un dernier pour la gouvernance « informatique et libertés », qui cible tous les responsables de traitement. Ces labels, présentés comme des « indicateurs de confiance », visent à inciter les organismes à se mettre en conformité. Dans son rapport, la Commission a également mis en avant les BCR, dans l'idée d'encourager les groupes à déployer des politiques de gestion des données personnelles.

2014 a également été marquée par la réalisation des premiers contrôles en ligne. Ainsi, 58 contrôles de ce type ont été menés entre octobre et décembre. La plupart d'entre eux portaient sur les *cookies*. Le nombre total de contrôles de la CNIL a dépassé la barre des 400 l'an passé (421).

Enfin, le nombre de plaintes a continué à augmenter, pour atteindre 5 825, dont 39% liées à Internet. Parmi elles, 150 concernaient un refus de référencement par les moteurs de recherche. En avril 2015, la CNIL a ouvert un nouveau service de plainte en ligne, qui devrait faciliter encore les démarches des personnes concernées.

Le projet de loi de santé réforme l'hébergement de données de santé

Projet de loi de modernisation de notre système de santé, adopté par l'Assemblée nationale et enregistré par le Président du Sénat le 15 avril 2015

Le 14 avril 2015, l'Assemblée nationale a adopté, en première lecture, le projet de loi de santé. Celui-ci comprend notamment une refonte du cadre législatif de l'hébergement de données de santé.

Le projet étend l'obligation de recourir à un hébergeur de données de santé (HDS) agréé au-delà des professionnels et des établissements de santé, pour l'élargir à toute personne physique ou morale produisant des données de santé. Afin de faciliter le recours aux prestataires d'hébergement, l'exigence de consentement préalable des personnes concernées à toute externalisation de leurs données de santé disparaît, en ne laissant subsister que le devoir d'information et le droit de s'opposer à tout moment pour des motifs légitimes. L'agrément des hébergeurs, actuellement prévu à l'article L.1111-8 du Code de la santé publique, est remplacé par une évaluation de conformité technique, réalisée par un organisme certificateur accrédité par le COFRAC. Cette certification porte sur les procédures, l'organisation et les moyens matériels et humains de l'hébergeur, ainsi que sur les modalités de qualification des applications hébergées. Ces évolutions vont dans le sens de la suggestion du Comité d'agrément des hébergeurs de données de santé (CAH), formulée dans son rapport d'activité 2012-2013, de « s'orienter vers une procédure de certification en s'inspirant de ce qui existe dans le domaine bancaire ».

L'équipe juridique HSC

juridique@hsc.fr

01 41 40 97 00

HSC BY DELOITTE

SASU au capital de 300 000 € - RCS Nanterre B 444 475 891 - Code NAF : 6202A

191 avenue Charles-de-Gaulle – F-92 200 NEUILLY-SUR-SEINE

Tél. : +33 (0)1 41 40 97 00 – Fax : +33 (0)1 41 40 97 09

Les prochaines formations juridiques HSC - 2015			
Formations principalement juridiques			
Correspondant informatique et libertés	Rennes, 8-10 juin	Strasbourg, 22-24 juin	Paris, 1-3 juillet
Essentiels juridiques pour gérer la SSI	Paris, 21-22 mai	Paris, 26-27 novembre	
Essentiels « informatique et libertés »	Paris, 13 novembre		
Formations comportant une partie juridique			
RGS v.2	Paris, 6 novembre		
RSSI	Paris, 5-9 octobre		
Sécurité du cloud computing	Paris, 21-23 septembre		
Tests d'intrusion avancés, exploits, hacking éthique (SANS SEC560)**	Paris, 19-23 octobre		

** : Formation certifiante

formations@hsc.fr, 01 41 40 97 04

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.

INFORMATIQUE ET LIBERTES

Conformément à l'article 32 de la loi n°78-17 du 6 janvier 1978, nous vous informons que les données à caractère personnel recueillies lors de votre abonnement font l'objet d'un traitement. Le responsable du traitement est la société Hervé Schauer Consultants. La finalité poursuivie par ce traitement est la constitution d'un fichier d'adresses de courrier électronique à des fins d'envoi périodique du bulletin d'actualités juridiques HSC. En application des articles 38 et suivants de la loi susmentionnée, vous disposez de droits d'opposition, d'accès et de rectification. Pour faire valoir ces droits, vous pouvez contacter le correspondant informatique et libertés d'HSC à l'adresse cil@hsc.fr.

HSC BY DELOITTE

SASU au capital de 300 000 € - RCS Nanterre B 444 475 891 - Code NAF : 6202A
191 avenue Charles-de-Gaulle – F-92 200 NEUILLY-SUR-SEINE
Tél. : +33 (0)1 41 40 97 00 – Fax : +33 (0)1 41 40 97 09