



CONSEQUENCES DES CONTROLES CNIL EN MATIERE DE VIDEOPROTECTION

Le client final peut-il se retourner contre l'installateur ?

- Dans quelle mesure un client final peut-il se retourner vers l'installateur quand la Cnil, lors d'un contrôle, constate une **non-conformité aux obligations légales** ?
- La responsabilité peut-elle être partagée, notamment dans le cadre d'un contrat de maintenance ? pour non-respect du masquage des zones privées, mauvais réglage ou encore dysfonctionnements pouvant affecter les dispositifs vidéo, comme l'absence d'enregistrement, la mauvaise qualité de l'image ?
- Rappelons que les contrôles effectués par la Cnil peuvent porter sur **l'ensemble des éléments du système** de la vidéoprotection, à savoir :
 - la qualité des données personnelles ;
 - le destinataire des images ;
 - leur durée de conservation ;
 - la sécurité des systèmes ;
 - la configuration des dispositifs au regard d'autorisations, l'information des personnes.
- **Seule la personne en charge du traitement est responsable** et encoure trois types de sanctions : des poursuites pénales, des sanctions administratives (annulation de l'autorisation préfectorale) et pécuniaires déterminées par la Cnil et d'éventuels dommages et intérêts, décidés devant les tribunaux.

Le client a une obligation de vérification

- Un recours contre l'installateur est possible, mais uniquement au titre des **préjudices subis**, comme l'atteinte à l'image de marque. Sa responsabilité ne sera toutefois pas facile à engager car l'installateur pourra prétendre que l'obligation repose, en premier lieu, sur les responsables du traitement.
- Toutefois, la mise en conformité d'un système suppose que le client ait une **obligation de vérification**.
- Ce qui signifie que, dans le cas d'un recours contre l'installateur, seule la **responsabilité civile** de ce dernier peut être engagée, et ce dans le cadre du **contrat de vente et d'installation**.
- Si le client a recetté le système, devront alors être distingués les éléments de **vices apparents** et les éléments de **vices cachés**.
- Rappelons que l'activité du fournisseur ou installateur est soumise à un cadre réglementaire strict (**certification**) (1), avec une quasi obligation de résultat, surtout dans le cadre de la mise en conformité.
- Ce qui n'exonère pas, pour autant, l'utilisateur de la nécessité de contrôler cette conformité. Ainsi, le fait que le fournisseur ou l'installateur soit certifié et soumis à des **obligations légales** n'est pas une cause d'exonération de l'obligation du client de procéder à un contrôle de conformité.

Les enjeux

Si la caméra ne respecte pas le plan, le client peut certes demander une mise en conformité avant la recette.

Mais s'il l'a recetté en l'état, les conséquences portent, avant tout, sur le fait d'avoir mis en œuvre une installation non conforme, plutôt que sur ses conséquences.

(1) Arrêtés du [3-8-2007](#) et du [5-1-2011](#).

Les conseils

L'obligation de conformité, vis-à-vis des pouvoirs publics, de la Cnil et des personnes concernées est une obligation incombant aux responsables du traitement.

La vigilance est donc de mise et une installation ne doit donc être recettée qu'après avoir vérifié sa conformité.

[ALAIN BENSOUSSAN](#)



Impact sectoriel : le Cil presse

LE CORRESPONDANT INFORMATIQUE ET LIBERTES DES ORGANISMES DE PRESSE

Un régime dérogatoire tenant compte du droit de la presse

- La loi Informatique et libertés accorde aux traitements mis en œuvre à des fins de journalisme professionnel un régime dérogatoire, afin de concilier la **liberté de la presse** avec la **protection des données** à caractère personnel (1).
- Il s'agit des traitements mis en œuvre par les organismes de **presse écrite** (papier ou en ligne) ou **audiovisuelle**, tel que les traitements de textes et d'images, les bases de données documentaires, l'archivage des contenus publiés.
- Les **articles** 6 5°, 8, 9, 22, 25-I 1° et 3°, 32, 39, 40 et 68 à 70 de la loi Informatique et libertés ne leur sont **pas applicables**. Ainsi donc :
 - les données à caractère personnel peuvent être conservées sans limitation de durée ;
 - les organismes de presse peuvent collecter et traiter des **données sensibles** (c'est-à-dire celles faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci), ou relatives à des infractions ou condamnations, sans avoir à recueillir le consentement des personnes concernée et la Cnil n'a pas à autoriser les fichiers contenant de telles données ;
 - les organismes de presse n'ont pas à **informer** les personnes dont les données sont collectées et traitées, des informations énumérées à l'article 32 (identité du responsable de traitement, finalité du traitement, données collectées, destinataires des données, etc.) ;
 - les personnes dont les données sont collectées et traitées ne peuvent pas exercer leurs **droits d'accès**, de rectification ou de suppression des données les concernant ;
 - les données à caractère personnel peuvent être librement **transférer** vers des Etats situés hors de l'Union européenne ; ces transferts ne font l'objet d'aucun encadrement spécifique et la Cnil n'a pas à les autoriser.

La désignation d'un Cil dispense de déclaration

- Les obligations Informatique et libertés non expressément exclues par l'article 67 s'appliquent aux traitements aux fins de journalisme professionnel.
- Ces traitements n'ont pas à être déclarés à la Cnil préalablement à leur mise en œuvre, **si l'organisme de presse a désigné un Cil**.
- Le Cil presse est nécessairement un salarié de l'organisme de presse ; il n'est toutefois pas obligatoire qu'il soit journaliste.
- Les articles 43 2°, 45, 48 4° et 7° et alinéas 10, 11 et 12, et 49, alinéa 5, du décret du 20 octobre 2005 ne sont pas applicables au Cil presse. Ainsi donc :
 - la **désignation** du Cil presse n'a pas à être portée à la connaissance des instances représentatives du personnel par le responsable de traitement préalablement à sa notification à la Cnil ;
 - la **liste des traitements** tenue par le Cil presse ne doit pas préciser le service chargé du droit d'accès ni la durée de conservation des données. En outre, cette liste ne peut pas être consultée ni communiquée à des tiers demandeurs ;
 - le Cil presse n'a pas à **informer** le responsable de traitement des manquements constatés avant toute saisine de la Cnil.

Les enjeux

Concilier la liberté de la presse avec la protection des données à caractère personnel.

(1) Art. 67 de la loi Informatique et libertés modifiée et art. 56 du décret du 20-10-2005.

Les conseils

Les organismes de presse n'ont pas à déclarer ces traitements mais doivent, en contrepartie, désigner un correspondant à la protection des données.

[VIRGINIE
BENSOUSSAN-BRULÉ](#)



Le futur de la vie privée, à horizon 2020 vu par 42 experts

- A l'occasion de la première journée d'études organisée par la Cnil sur les enjeux et la régulation de la **vie privée sur internet à l'horizon 2020** (1), la Cnil a diffusé le premier numéro des cahiers innovation & prospective.
- Dans ce premier numéro, la Cnil s'est penchée sur « le futur de la vie privée, à l'horizon 2020 » et a donné la parole à **42 experts** (2).
- Pour la plupart des experts, il faudrait adapter notre régulation, voire, pour **Alain Bensoussan**, songer même à écrire une **loi des droits fondamentaux du numérique**.
- Les règles et les valeurs qui ont cours dans le monde « réel » doivent s'appliquer également au **monde virtuel**. Il faut non seulement adapter notre régulation, mais songer à écrire une loi des droits fondamentaux du numérique.

Protection des données à caractère personnel en Nouvelle-Zélande

- Dans sa décision du **19 décembre 2012** (2), la Commission Européenne a reconnu le caractère adéquat de la protection des données à caractère personnel mise en œuvre par la Nouvelle-Zélande.
- Ainsi, les données à caractère personnel pourront désormais être transférées des 27 pays membres de l'UE et des 3 pays membres de l'EEE vers la Nouvelle-Zélande sans qu'il ne soit nécessaire de prévoir d'autres garanties.
- L'objectif de la Commission Européenne est de faciliter la libre circulation des données à caractère personnel et de ce fait les échanges économiques entre l'Union-Européenne et la Nouvelle-Zélande, les échanges de biens entre elles s'élevant à près de 6,7 milliards d'euros par an et le commerce de services à 3,1 milliards.

Exploiter le potentiel de l'informatique en nuage en Europe

- Un avis du Contrôleur européen de la protection des données (CEPD) du **16 novembre 2012** a été adopté sur les actions clés et les mesures visant à accélérer l'utilisation de services de Cloud computing en Europe (3).
- L'avis du CEPD aborde les défis pour la protection des données engendrés par le Cloud et la façon dont la proposition de règlement de protection des données y répondra lorsque les règles révisées entreront en vigueur.

Sources

(1) [Conférence Cnil Vie Privée 2020](#).

(2) [Cnil-CAHIERS IP numéro 1](#), décembre 2012.

(2) [Communiqué presse IP-12-1403_FR](#), Bruxelles le 19-12-2012.

(3) [Site du CEPD](#) – Avis (30 p.) et Communiqué (2 p.) du 16-11-2012.

La JTIL est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 29, rue du colonel Pierre Avia 75015 Paris, président : Alain Bensoussan

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier.

Diffusée uniquement par voie électronique – gratuit – ©Alain Bensoussan 2012

ISSN 1634-0698

Abonnement à partir du site : <http://www.alain-bensoussan.com/outils/abonnement-juristendance>

Les FAQ juristendances

POINT D'ETAPE ET CALENDRIER PREVISIONNEL SUR LE PROJET DE REGLEMENT EUROPEEN

Que prévoit le projet de règlement ?

- Le projet de règlement (1) prévoit de **réformer la Directive** européenne de 1995 appelée à être remplacée. Il devrait notamment permettre une meilleure **harmonisation** et renforcer l'effectivité des règles de protection des données personnelles avec **l'essor du numérique**.
- Les **droits des citoyens** sont en grande partie **renforcés** : reconnaissance d'un droit à l'oubli, d'un droit à la portabilité de leurs données et clarification des règles relatives au recueil du consentement et à l'exercice de leurs droits.

Où en est le projet de texte ?

- Depuis juillet 2012, le projet de texte est **en cours d'examen par le Parlement européen** au sein de la Commission chargée des questions relatives aux affaires civiles, justice et affaires intérieures (Commission LIBE) et sous l'égide de la Présidence chypriote du Conseil de l'Union européenne via le Groupe de travail chargé des questions concernant les échanges d'informations et la protection des données (DAPIX).
- La Commission vient d'accueillir le projet de rapport du Parlement européen sur la protection des données le **10 janvier 2013** (2).
- Le texte définitif devrait être adopté **début 2014**. Il prévoit que les entreprises disposent d'une **période transitoire de deux ans** pour se mettre en conformité.

Quelle est la position du « G29 », groupe des Cnil européennes ?

- Le G29 a rendu un premier **avis** sur la proposition de projet de Règlement en **mars 2012** suivi par un second avis en **octobre 2012** (3).
- Ces avis contiennent des **propositions d'amélioration** concernant, notamment, la définition de données personnelles, la notion de consentement, les actes délégués et d'application, les dérogations aux transferts internationaux de données, la notification des failles de sécurité et le droit à l'oubli, afin d'alimenter les discussions législatives au sein des instances européennes.
- Le G29 a souligné la nécessité, pour mettre en œuvre le concept de **guichet unique** souhaité par la Commission pour les entreprises, d'une autorité chef de file coopérant avec les autres autorités compétentes pour superviser les traitements de données mis en œuvre dans les Etats Membres.

Le Cil obligatoire : quelles seront ses modalités d'organisation ?

- La **Cnil** dresse un premier **portrait synthétique** de ce que pourraient être le statut et les missions des futurs délégués à la protection des données (DPD). Même si tout peut encore changer, de grandes tendances apparaissent (4).
- Ces orientations doivent encore être validées par le Parlement européen et le Conseil de l'Union européenne.

Références

(1) [Proposition de règlement 2012-0011 \(COD\) 25-1-2012.](#)

Une fois adopté, le règlement européen sera d'application directe dans l'ensemble des États Membres de l'Union européenne.

(2) [Memo EN 13/4](#), European Commission, Brussels 10 January 2013.

(3) [Avis 01/2012](#) du 23-3-2012 et [avis 08/2012](#) du 5-10-2012 (en anglais).

(4) Le CIL à l'heure du projet de règlement européen, [site Cnil](#), article du 5-4-2012.



Prochains événements

Open innovation et Propriété intellectuelle : enjeux et risques : 16 janvier 2013

- **Laurence Tellier-Loniewski**, directeur du pôle propriété intellectuelle et **Claudine Salomon**, directeur du département Droit et Politique industrielle animeront aux côtés d'**Anne Laurent** directrice du service juridique de Propriété intellectuelle Europe du groupe Salomon [Amer Sports](#), un petit-déjeuner débat consacré aux enjeux et risques de l'open innovation.
- L'open innovation née du développement des réseaux sociaux et des pratiques collaboratives offre aux entreprises une réelle opportunité de profiter de l'intelligence collective d'une communauté de contributeurs.
- Cette pratique qui connaît un engouement certain dans le monde industriel n'est toutefois pas dénuée de risques au regard des droits de propriété intellectuelle que l'entreprise initiatrice pourrait revendiquer.
 - Comment appréhender les problématiques juridiques de l'open innovation ?
 - En particulier comment concilier la protection des idées, des concepts, du savoir-faire, des inventions brevetables, des innovations protégées par le droit d'auteur, des dessins et modèles, et des marques avec le monde de l'open innovation ?
 - Comment mettre en place une politique de l'open innovation en préservant la confidentialité d'une innovation, sa traçabilité et sa validité ?
 - Comment anticiper les risques de contrefaçon ?
 - Comment organiser une architecture contractuelle appropriée et prévoir une contrepartie équitable ?
 - Plus généralement comment mettre en place une organisation pertinente en utilisant des outils contractuels et des outils internes adaptés à l'open innovation ?
- Telles sont les questions qui seront abordées lors de ce petit-déjeuner.
- Le petit-déjeuner débat aura lieu le 16 janvier 2013 de 9 heures à 11 heures (accueil à partir de 8 heures 30), dans les locaux du [29, rue du Colonel Avia 75015 Paris](#).
- **Inscription gratuite** sous réserve de confirmation avant le 11 janvier 2013 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit-déjeuner à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le [Bulletin inscription](#) joint au 01 41 33 35 36.

Vidéoprotection et contrôles Cnil : quelles responsabilités des grands acteurs et utilisateurs finaux ? : 30 janvier 2013

- **Alain Bensoussan** animera aux côtés de **Michel George**, Président du [GPMSE](#) Installation (Groupement professionnel des métiers d'installateurs mainteneurs en sécurité électronique) et de **Virginie Cadieu**, Directrice Marketing et communication du groupe [Aasset Security International](#) (ASI), membre du groupe TKH et partenaire historique du GPMSE, un petit-déjeuner débat consacré à la vidéoprotection et aux contrôles Cnil.
- Des textes spécifiques encadrent les dispositifs de vidéoprotection selon qu'ils sont installés sur la voie publique, au travail, dans un magasin, des locaux professionnels, un établissement scolaire, un immeuble d'habitation ou à son propre domicile.
 - Quelles sont les différentes règles applicables ? (autorisation, déclaration, agrément, certification, etc.)
 - Quelles sont les précautions à prendre lors de l'installation d'un dispositif de vidéoprotection ?
 - Qui sont les personnes habilitées à visionner les images enregistrées ?
 - Peut-on associer la reconnaissance faciale (système biométrique) à un dispositif de vidéoprotection ?
 - Pendant combien de temps peut-on conserver les images ?
 - Quel est le rôle respectif des acteurs du secteur de la vidéoprotection (préfecture, commission départementale, CNV, Cnil, comité d'entreprise, collectivités locales, installateurs, responsables sécurité...)?
 - Quels sont les outils appropriés pour mieux relayer l'information auprès des entreprises ? (charte, guide etc.)
- Telles sont les questions qui seront abordées lors de ce petit-déjeuner.
- Le petit-déjeuner débat aura lieu le 30 janvier 2013 de 9 heures à 11 heures (accueil à partir de 8 heures 30), dans les locaux du [29, rue du Colonel Avia 75015 Paris](#).
- **Inscription gratuite** sous réserve de confirmation avant le 21 janvier 2013 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit-déjeuner à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le [bulletin d'inscription](#) en ligne au 01 41 33 35 36.



Formations intra-entreprise : 1^{er} semestre 2013

Le cabinet a la qualité d'organisme de formation professionnelle depuis 30 ans¹.

Il a en outre obtenu le label Cnil « [Lexing® formation informatique et libertés](#) » pour son catalogue de formations informatique et libertés.



Informatique et libertés

- [Informatique et libertés \(niveau 1\)](#) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires. 11-01 ; 29-03 et 07-06-2013
- [Cil \(niveau 1\)](#) : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre. 18-01 ; 15-03 et 21-06-2013
- [Informatique et libertés secteur bancaire](#) : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire. 22-01 ; 28-03 et 11-06-2013
- [Informatique et libertés collectivités territoriales](#) : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés. 25-01 ; 8-03 et 14-06-2013
- [Sécurité informatique et libertés](#) : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité. 22-02 et 28-06-2013
- [Devenir Cil](#) : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.). 08-02 et 05-04-2013
- [Cil \(niveau 2 expert\)](#) : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design. 13-02 et 24-04-2013
- [Informatique et libertés gestion des ressources humaines](#) : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines. 15-02 et 12-04-2013
- [Flux transfrontières de données](#) : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi. 22-02 et 19-04-2013
- [Contrôles de la Cnil](#) : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle). 26-02 et 23-04-2013
- [Informatique et libertés secteur santé](#) : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité. 01-03-2013
- [Formation intra entreprise Informatique et libertés à l'attention du comité exécutif](#) : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité. Selon demande

¹ Catalogue de nos formations 2013 sur : <http://www.alain-bensoissan.com/secteurs-dactivites/formation-intra-entreprise>



5^e édition : Informatique, Télécoms, Internet (actualisée au 10-09-2012)

▪ Comme pour les quatre premières éditions, l'ouvrage expose toutes les règles juridiques à connaître applicables à l'économie des systèmes d'information et confronte le monde de l'informatique :

- au droit du travail (contrôle des salariés, évaluation professionnelle, etc.) ;
- à la fiscalité (conception et acquisition de logiciels, crédit d'impôt recherche, avantages de l'infogérance, etc.) ;
- aux assurances ;
- au domaine de la santé (carte santé et secret médical, etc.) ;
- à internet et au commerce électronique.

▪ Cette nouvelle édition intègre toutes les nouveautés les plus récentes et notamment :

- les nouveaux contrats d'externalisation (de la virtualisation au cloud computing) ;
- le nouveau CCAG des marchés de l'information et de la communication (TIC) ;
- le nouveau régime de la vidéoprotection issu de la LOPPSI 2 ;
- la E-réputation de l'entreprise (blogs et réseaux sociaux) ;
- la régulation des activités commerciales sur internet ;
- le téléchargement illégal sur internet ;
- l'usurpation d'identité numérique, la régulation des activités commerciales sur internet, etc.

▪ Cette nouvelle édition innove en ajoutant les référentiels normatifs qui font pleinement partie du cadre juridique applicable aux différents systèmes qui traitent l'information : référentiels de système de management de la qualité, de l'environnement et de la sécurité ou d'ingénierie logicielle (CMMI, ISO 20000-1, ITIL, famille ISO 9000, etc.).

▪ Les mises à jour apportées à l'édition 2012 de l'ouvrage Informatique, Télécoms, Internet sont [disponibles en ligne](#).



[Informatique,](#)
[Télécoms, Internet,](#)
Editions Francis
Lefebvre 5e éd. 2012

² Nos publications : <http://www.alain-bensoussan.com/espace-publication/bibliographie>