



**UCOPIA COMMUNICATIONS : LA RÉPONSE AUX OBLIGATIONS  
LÉGALES POUR LES ORGANISATIONS OFFRANT UN ACCÈS  
À L'INTERNET AU PUBLIC**





## 2 SOMMAIRE

1. Contexte
2. Zoom : ce que vous devez savoir sur la loi contre le terrorisme & autres dispositions légales en 5 points
3. Ne pas conserver certaines données de connexions : un risque juridique
4. Une réponse adaptée : notre portail captif
5. Nos principaux déploiements médiatiques en 2010
6. A propos d'UCOPIA Communications



## 3 1. CONTEXTE

### Offrir un accès à l'internet au public n'a rien d'anodin.

Depuis une loi n°2006-604 du 23 janvier 2006 relative à la lutte contre le terrorisme, les cafés, hôtels, cybercafés, restaurants, aéroports, mais aussi toutes les personnes qui offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont tenues de conserver un certain nombre de données dites de trafic.

Le présent livre a notamment pour but d'alerter ces personnes qui, faute d'avoir conscience des obligations auxquelles elles sont tenues, offrent, bien souvent à leurs clients, une

connexion permettant une communication à l'internet sans avoir pris le soin de mettre préalablement en place le dispositif qui leur permettra de transmettre, à qui de droit, les informations qu'elles étaient pourtant tenues de conserver.

Parce que ces différentes obligations sont notamment assorties de sanctions pénales, il apparaît nécessaire de les détailler.

Sadry Porlon, avocat au Barreau de Paris. Docteur en droit, il est également chargé d'enseignement au sein d'une école de commerce, notamment en droit des médias et de la communication ainsi qu'en droit du commerce électronique et du multimédia.

	Loi contre le terrorisme & autres dispositions légales	Loi HADOPI
L'opérateur de communications électroniques est tenu de conserver...	<ul style="list-style-type: none"> <li>Les informations permettant d'identifier l'utilisateur</li> <li>Les données relatives aux équipements et terminaux utilisés</li> <li>Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication</li> <li>Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs</li> <li>Les données permettant d'identifier le ou les destinataires de la communication</li> </ul> <p>(Décret n°2006-358 du 24 mars 2006, article R. 10-13 du CPCE)</p>	
L'opérateur de communications électroniques ne doit pas conserver...	<p>« le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications »</p> <p>(Article L. 34-I-V du CPCE)</p>	
Les sanctions en cas de non respect de l'obligation de conservation des données sont...	<p>Un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques et 375.000 euros pour les personnes morales.</p> <p>(Article L. 39-3 du CPCE)</p>	
La durée de conservation des données est...	<p>D'un an pour le cas de la conservation des données relatives au trafic lorsqu'il s'agit de la recherche, de la constatation et de la poursuite des infractions.</p> <p>(Le décret du 24 mars 2006 prévoit des durées de conservations variables en fonction des finalités).</p>	

Des données à délivrer aux personnes habilitées à les recevoir sous peine de sanctions pénales...	<p>Les données conservées par l'opérateur de communications électroniques ne peuvent être transmises qu'à des personnes habilitées parmi lesquelles :</p> <ul style="list-style-type: none"> <li>L'officier de police judiciaire au cours d'une enquête de flagrance</li> <li>le Procureur de la République ou l'officier de police judiciaire sur autorisation du procureur et au cours d'une enquête préliminaire</li> <li>le juge d'instruction ou l'officier de police judiciaire par lui commis au cours de l'instruction</li> <li>les agents individuellement habilités des services de police et de gendarmerie, spécialisés dans la prévention des actes de terrorisme</li> </ul> <p>(Articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale ainsi que l'article L. 34-1-1 du CPCE)</p> <p>L'article L. 39-4 du CPCE précise que : «sera puni de trois mois d'emprisonnement et de 30.000 euros d'amende ou de l'une de ces deux peines seulement quiconque aura, sans raison valable, refusé de fournir les informations ou documents ou fait obstacle au déroulement de l'enquête ».</p>	<p>La commission de protection des droits de la HADOPI peut demander à l'opérateur de communications électroniques de lui remettre :</p> <ul style="list-style-type: none"> <li>nom de famille, prénoms ;</li> <li>Adresse postale et adresses électroniques ;</li> <li>Coordonnées téléphoniques ;</li> <li>Adresse de l'installation téléphonique de l'abonné</li> </ul> <p>(Décret n° 2010-236 du 5 mars 2010 en son article 2)</p> <p>« Est puni de l'amende prévue pour les contraventions de cinquième classe (soit 1.500 euros) le fait de contrevenir aux dispositions de l'article R. 331-37 » à savoir, pour l'opérateur de communications électroniques, de ne pas communiquer les données à caractère personnel et les informations mentionnées au 2° de l'annexe du décret n° 2010-236 du 5 mars 2010 qui lui seront réclamées.</p> <p>(Article R. 331-38 du décret n° 2010-872 du 26 juillet 2010)</p>
---	---	--



#### UN RISQUE JURIDIQUE



Au sens de la Directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques du commerce électronique dans le marché intérieur dite « Directive sur le commerce électronique » et surtout de la Loi de Confiance dans l'Economie Numérique du 21 juin 2004 qui est venue transposer ladite directive en France, un fournisseur d'accès est un intermédiaire technique au même titre qu'un fournisseur d'hébergement <sup>1</sup>.

L'article 6-I- 1 de la Loi n° 2004-575 de Confiance dans l'Economie Numérique (ci-après LCEN) définit les fournisseurs d'accès comme: « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne (...) ».

L'article 6-II de la LCEN du 21 juin 2004 impose aux fournisseurs d'accès la conservation des données « de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elle est prestataire ».

La justification de cette obligation tient notamment au fait que pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, l'autorité judiciaire

1. Celui qui assure pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux d'écrits, d'images de sons ou de messages de toute nature fournis par les destinataires de ces services.

doit être en mesure de se faire remettre ces données et, le cas échéant, pouvoir identifier l'internaute indélicat qui en est l'auteur.

Nous verrons successivement les obligations de conservation de données auxquelles sont tenus les opérateurs de communications électroniques, la nature des données qu'ils sont tenus de conserver, la durée de la conservation desdites données, les personnes qui sont habilitées à leur réclamer la communication de ces éléments d'information, mais aussi les sanctions qui peuvent accompagner le non-respect de ces différentes obligations.

#### Des opérateurs de communications électroniques tenus à une obligation de conservation des données de connexion

La loi n°2006-604 du 23 janvier 2006 relative à la lutte contre le terrorisme a étendu l'obligation de conserver des données à l'ensemble des personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit et non plus à ceux dont l'activité était d'offrir un accès à des services de communication au public en ligne.

L'article L. 34-1 du Code des Postes et des Communications Electroniques (ci-après CPCE) modifié, une première fois, par la loi susvisée dispose, en effet, que « les personnes qui, au titre d'une activité professionnelle principale ou accessoire offrent au public une connexion permettant une communication au public en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article ».



Sont désormais tenus à des obligations similaires en termes de conservation des données, aussi bien les fournisseurs d'accès à internet classiques (comme Orange, SFR ou Free) que ceux qui offrent un accès à internet à titre occasionnel et temporaire comme les hôtels, cafés, aéroports, universités, restaurants et tout autre endroit qui propose un accès au réseau internet au public.

Cette dernière précision permet d'ailleurs d'exclure les entreprises et les administrations fournissant un accès internet à leurs employés de cette obligation de conservation prévue par la loi du 23 janvier 2006.

#### Quid des données à conserver ?

##### Celles qu'ils sont tenus de conserver

L'article L. 34-1 du CPCE, modifié par la loi du 23 janvier 2006, indiquait qu'un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, déterminerait les catégories de données à conserver.

Le Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques en son article R. 10-13 du CPCE décrit les catégories de données qui devront être conservées par l'opérateur de communications électroniques comme étant :

- Les informations permettant d'identifier l'utilisateur

- Les données relatives aux équipements et terminaux utilisés
- Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs
- Les données permettant d'identifier le ou les destinataires de la communication

Ces informations constituent donc le minimum nécessaire aux personnes habilitées à la recherche, à la constatation et à la poursuite des infractions pénales.

##### Celles qui sont exclues de l'obligation de conservation

L'article L. 34-I-V du CPCE précise que l'obligation de conservation des données conservées porte « exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux » et « ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

« La conservation et le traitement de ces données devant par ailleurs se faire dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés » ajoute ce même article.

## La question des données permettant l'identification de l'utilisateur

En l'état, il apparaît que l'obligation de conservation des données impose aux opérateurs de communications électroniques qu'ils conservent notamment « *les éléments permettant l'identification* », mais ne leur impose pas expressément de connaître et donc de conserver l'état civil (nom et prénom) des utilisateurs de leurs services.

Le décret du 24 mars 2006 n'oblige donc pas les opérateurs de communications électroniques comme les hôtels, restaurants, cybercafés et autres aéroports de demander aux utilisateurs de l'accès à internet qu'ils mettent à leur disposition de s'identifier par le biais de leur état civil.

Dès lors, et en attendant qu'un arrêté vienne préciser le périmètre des « *données permettant l'identification* » évoquées dans le décret, l'obligation à laquelle ils sont tenus consiste uniquement à recueillir les informations d'ordre général qui permettront d'identifier l'utilisateur.

Là où le fournisseur d'accès classique est pleinement en mesure de communiquer le nom et le prénom de ses abonnés, celui qui, comme un hôtel ou un café, ne fournit un accès à internet à ses clients qu'à titre temporaire peut donc très bien le faire sans leur demander de s'identifier de façon nominative.

Cependant, et c'est là, l'un des aspects à ne pas méconnaître, si ces opérateurs de communications électroniques venaient à solliciter les noms et prénoms de leurs utilisateurs spontanément, ils seraient tenus, au même titre que les fournisseurs d'accès dits classiques, de conserver ces « éléments permettant l'identification » qu'ils se seront alors procurés.

## La loi HADOPI doit pousser à la prudence l'opérateur de communications électroniques

La loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (dite HADOPI 1) qui en son article 14 a modifié, à son tour, l'article L. 34-1 du CPCE de façon à permettre aux opérateurs de communications électroniques de communiquer à la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (ci-après la HADOPI) les données à caractère personnel et informations relatives à leurs abonnés recueillies en application du décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel.

Ce décret précise en son article 2 que les données à caractère personnel et informations enregistrées dans le cadre de la mise en œuvre, par la commission de protection des droits de la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet, de la procédure de recommandations prévue par l'article L. 331-25 du code de la propriété intellectuelle figurent en annexe au présent décret.

Il s'agit des données suivantes :

- nom de famille, prénoms ;
- adresse postale et adresses électroniques ;
- coordonnées téléphoniques ;
- adresse de l'installation téléphonique de l'abonné



Les hôtels, restaurants et autres cybercafés qui fournissent l'accès à internet à leurs clients ont donc ceci de particulier qu'ils ne seront parfois pas en mesure de communiquer à la commission de protection des droits de la HADOPI, notamment, les noms et prénoms des utilisateurs de leurs services, faute de leur avoir demandé ces éléments d'information.

Ce sont d'ailleurs bien souvent des opérateurs de communications électroniques au sens de la loi n°2006-604 du 23 janvier 2006, au motif qu'ils offrent, au titre d'une activité professionnelle principale ou accessoire, au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, mais également des abonnés au réseau internet d'un fournisseur d'accès classique (Orange, Free ou encore SFR).

Dès lors, nous ne saurions trop conseiller à ces opérateurs de communications électroniques « à la double casquette » de solliciter spontanément l'indication de leur état civil aux utilisateurs de leurs services, dans le strict respect des dispositions de la loi n° 78-17 du 6 janvier 1978, de façon à les responsabiliser, mais aussi de rester attentifs à la mise en place prochaine des outils de sécurisation des réseaux internet.

Le gouvernement a d'ailleurs publié au Journal Officiel du 26 décembre 2010, un décret portant sur la labellisation des outils de sécurisation ; première étape qui permet aux fournisseurs de solutions de se porter candidat au label avant qu'une seconde portant sur les spécifications fonctionnelles de ces moyens ne viennent

entériner la mise en place de tels outils ; lesquels devraient (c'est l'objectif affiché) empêcher tout téléchargement illégal par le biais du réseau internet de l'opérateur/abonné.

## Des données à conserver pendant...

Le décret du 24 mars 2006 prévoit des durées de conservations variables en fonction des finalités.

Une durée fixe d'un an pour le cas de la conservation des données relatives au trafic lorsqu'il s'agit de la recherche, de la constatation et de la poursuite des infractions. Une durée qui commence à courir à compter de l'enregistrement des données.

Une durée variable de conservation est prévue à l'article R. 10-14, III du CPCE pour les données nécessaires à la facturation et à la commercialisation des services. Elle est intimement liée à la nécessité de l'opération en cause mais ne pourra en tout état de cause excéder un an. Cette durée correspond à la limite visée à l'article L. 34-2 qui prévoit une prescription d'un an à compter de l'exigibilité de la dette.

Une durée variable est également prévue pour la conservation en vue d'assurer la sécurité des réseaux, laquelle ne pourra toutefois dépasser trois mois (article L. 34-1 III alinéa 2 du CPCE).

Après ces différentes périodes, les données devront avoir fait l'objet d'une anonymisation.

## ...sous peine de sanctions pénales

Tout manquement à l'obligation de conservation des données expose la personne à laquelle incombe cette obligation aux sanctions visées à l'article L. 39-3 du CPCE soit un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques et 375.000 euros pour les personnes morales conformément à l'article 131-18 du Code pénal qui dispose que « le taux maximum applicable aux personnes morales est égale au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ».

## Des données à délivrer aux personnes habilitées...

Les données conservées par l'opérateur de communications électroniques ne peuvent être transmises qu'à des personnes habilitées.

Conformément aux articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale, l'officier de police judiciaire au cours d'une enquête de flagrance, le procureur de la République ou l'officier de police judiciaire sur autorisation du procureur et au cours d'une enquête préliminaire, ainsi que le juge d'instruction ou l'officier de police judiciaire par lui commis au cours de l'instruction peuvent « par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel ».

L'article L. 34-1-1 du CPCE prévoit également que certains agents individuellement habilités des services de police et de gendarmerie, spécialisés dans la prévention des actes de terrorisme puissent exiger des opérateurs la communication des données concernées et traitées par ces derniers conformément à

l'article 34-1 du Code précité.

Comme nous avons pu le voir précédemment, il faut également ajouter à cette liste de personnes habilitées à recevoir les données de trafic, la Commission de protection des droits de la HADOPI.

## ...sous peine de sanctions pénales

L'article L. 39-4 du CPCE précise que : « sera puni de trois mois d'emprisonnement et de 30.000 euros d'amende ou de l'une de ces deux peines seulement quiconque aura, sans raison valable, refusé de fournir les informations ou documents ou fait obstacle au déroulement de l'enquête ».

L'article R. 331-38 du décret n° 2010-872 du 26 juillet 2010 relatif à la procédure devant la commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet dispose quant à lui qu' : « Est puni de l'amende prévue pour les contraventions de cinquième classe (soit 1.500 euros) le fait de contrevenir aux dispositions de l'article R. 331-37 » à savoir, pour l'opérateur de communications électroniques, de ne pas communiquer les données à caractère personnel et les informations mentionnées au 2° de l'annexe du décret n° 2010-236 du 5 mars 2010 qui lui seront réclamées.

## CONCLUSION

Ce tour d'horizon des obligations légales auxquelles sont tenues les personnes morales ou physiques qui offrent un accès à l'internet au public doit avoir pour conséquence d'alerter ces dernières sur les risques juridiques existant et les précautions à prendre en la matière.

## 4. UNE RÉPONSE ADAPTÉE :

### NOTRE PORTAIL CAPTIF

La solution UCOPIA répond aux besoins des organisations souhaitant s'équiper d'une connexion Internet sécurisée (Wi-Fi en libre accès, connexion invités...) afin d'être en conformité avec la loi contre le terrorisme de 2006.

Ces solutions, à destination notamment :

- des entreprises,
- des hôtels,
- des établissements d'enseignement,
- des hôpitaux,
- des points de vente,
- ou encore des administrations,

permettent aux utilisateurs de se connecter de manière sécurisée au réseau et d'utiliser les applications métier et l'Internet de façon simple et sûre.

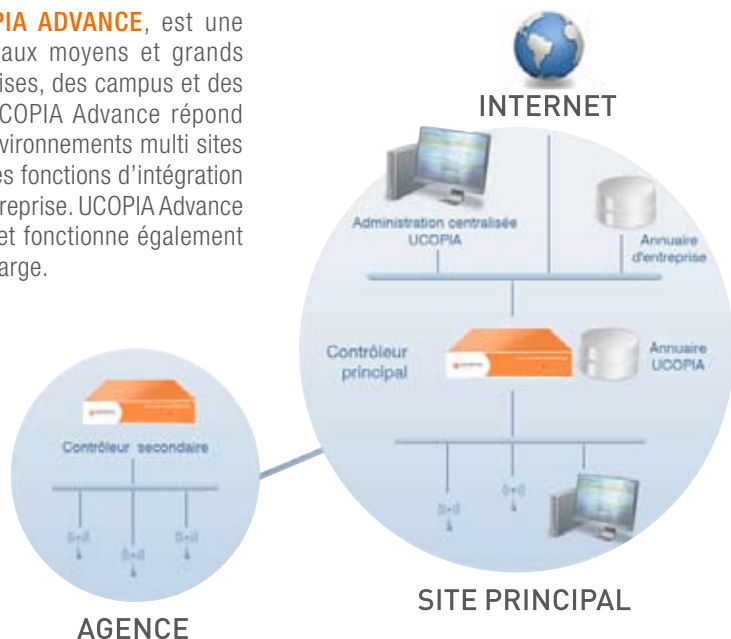
L'offre UCOPIA se décompose en deux gammes : Advance et Express.



### LA GAMME UCOPIA EXPRESS

se présente sous la forme d'une solution prête à l'emploi parfaitement adaptée aux besoins des hôtels, cliniques, établissements d'enseignement secondaires et PME en général.

**LA GAMME UCOPIA ADVANCE**, est une solution destinée aux moyens et grands projets des entreprises, des campus et des administrations. UCOPIA Advance répond aux besoins des environnements multi sites et propose toutes les fonctions d'intégration avec le LAN de l'entreprise. UCOPIA Advance peut être redondé et fonctionne également en répartition de charge.



## LES PRINCIPAUX AVANTAGES DE LA SOLUTION

- La sécurité combinant l'authentification, le contrôle d'accès par profil et la traçabilité des connexions
- La simplicité de mise en œuvre et d'administration
- Une gestion précise des indicateurs de performance
- Le confort d'utilisation (multi portails d'accueil)
- L'accès zéro configuration (pas besoin d'assistance technique)
- Un portail captif totalement personnalisable
- Des coûts d'exploitation réduits de 90%
- Un retour sur investissement < 6 mois
- Une gamme complète et évolutive (de 5 à plus de 1000 connexions simultanées)
- Une gestion des accès adaptée à toutes les situations
  - Par auto-enregistrement et envoi des identifiants par SMS ou mails
  - Par auto-enregistrement et paiement par paypal
  - Par un administrateur délégué (hôtesse d'accueil...)
  - Par auto-enregistrement simple

Nos deux solutions se placent entre un réseau d'accès filaire (ethernet, dslam, CPL) ou sans fil (Wi-Fi) et le LAN de l'organisation.

Tous les flux en provenance ou à destination de l'utilisateur traversent le boîtier de façon à garantir la sécurité, simplifier le couplage avec le LAN, faciliter l'administration, et améliorer le confort des utilisateurs.

Suivant le modèle, nos solutions peuvent gérer de 5 à plus de 1000 utilisateurs simultanés et s'installent très simplement dans l'infrastructure réseau. Les performances techniques, la simplicité de mise en service, le respect rigoureux de la réglementation font de notre contrôleur le produit de référence actuel.

### UCOPIA est le seul produit combinant

- L'analyse des flux (Qui fait Quoi, Quand et Comment)
- Une base de données dédiée au stockage des journaux de connexion, à la consultation et à l'analyse
- Un disque local et une sauvegarde en ligne automatique pour l'archivage des journaux



## 5. NOS PRINCIPAUX DÉPLOIEMENTS MÉDIATIQUES EN 2010

### LE TOUR DE FRANCE

UCOPIA gère depuis plusieurs années les accès, la qualité de service et l'administration des connexions Wi-Fi du Tour de France. Un programme qui concerne la connexion journalière de près de 1 500 personnes (journalistes et équipes techniques présents sur le Tour).

### LA POSTE

125 bureaux de poste sont équipés sur le territoire national principalement dans les zones rurales, les 2 contrôleurs UCOPIA sont hébergés à Nantes et à Bordeaux, l'architecture est ainsi centralisée.

### LA MAIRIE DE MEGÈVE

bénéficie d'un accès Internet totalement sécurisé permettant une gestion centralisée des tickets identifiants délivrés par l'office du tourisme et la médiathèque, mais également la gestion autonome à travers l'envoi gratuit aux utilisateurs d'un sms lors de leur première connexion sur le portail dédié.

### L'AÉROPORT DE NICE CÔTE D'AZUR

La solution choisie, fournit jusqu'à 200 connexions simultanées au sein de l'aéroport permettant d'être en conformité avec la loi anti-terroriste et offre ainsi aux passagers une solution de qualité, fiable, sécurisée, évolutive & performante.

### RÉSIDE ÉTUDES

120 résidences étudiantes équipées sur le territoire national avec un déploiement de 120 contrôleurs UCOPIA (Express 300), plus de 12 millions de connexions par an.

## 6. À PROPOS D'UCOPIA COMMUNICATIONS

Créée en 2002, UCOPIA Communications est leader sur le marché des contrôleurs d'accès visiteurs & nomades.

UCOPIA est une solution certifiée par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) qui assure la mission d'autorité nationale en matière de sécurité des systèmes d'information.



UCOPIA Communications commercialise son offre en s'appuyant sur un réseau européen de plusieurs centaines d'intégrateurs, experts dans les domaines des réseaux, de la convergence IP et de la sécurité, mais aussi spécialisés sur des secteurs d'activités (hospitalité, éducation, PME...).

Grâce à l'expertise de ce réseau de partenaires, UCOPIA peut conseiller et accompagner ses clients dans leurs projets, quels que soient leur taille et leur secteur d'activité.

### UCOPIA COMMUNICATIONS EN QUELQUES CHIFFRES

- Plus de **4000 clients** dans tous les secteurs
- Un réseau de plus de **150 partenaires**
- 58 millions d'utilisateurs** en 2010 sur nos portails
- Un chiffre d'affaires en progression de **25 %** en France avec un **doublent** à l'international



En 2010, UCOPIA a équipé plus de :

350  
hôtels

120  
établissements  
de santé

80  
établissements  
scolaires

120  
établissements  
publics

200  
PME et  
grands comptes

Vous trouverez ci-dessous une brève sélection de nos clients qui ont choisi de nous faire confiance pour leur sécurité.



**UCOPIA Communications :**  
**la réponse aux obligations légales**  
**pour les organisations offrant un**  
**accès à l'Internet au public**



- ✘ Quelles sont les obligations des personnes qui offrent un accès à l'internet au public ?
- ✘ Quelles précautions doivent-elles prendre ?
- ✘ Quelles données doivent-elles s'assurer de conserver ? À quoi s'exposent-elles si elles ne les conservent pas ?
- ✘ Combien de temps doivent-elles être conservées ?
- ✘ À qui doivent-elles les transmettre ?
- ✘ À quoi s'exposent-elles si elles ne les transmettent pas ?

*Voici quelques unes des questions auxquelles se propose de répondre le présent livre blanc...*

*Ecrit par Me Sadry Porlon, Avocat au barreau de Paris*

*Coordonné par Vanessa Pouzet, Responsable marketing UCOPIA Communications*