UCOPIA
COMMUNICATIONS

UCOPIA COMMUNICATIONS :
La réponse aux obligations légales pour les organisations offrant un accès à l'internet au public en France et dans les Etats membres de l'Union Européenne.

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 | Transposition de la directive 2006/24/CE et durées de conservation des données imposées par les Etats membres

5 | LA CNIL

6 | Les principes de la charte Internet

7 | Une réponse adaptée : les solutions UCOPIA

8 | Nos principaux déploiements médiatiques en 2012

9 | À propos d'UCOPIA Communications

1 | CONTEXTE

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

Depuis une loi n°2006-64 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, en effet, 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.

Une directive 2006/24/CE en date du 15 mars 2006 contraint également l'ensemble des Etats membres de l'Union européenne à adopter une loi obligeant les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication de conserver les données relatives aux communications pour une durée comprise entre 6 et 24 mois.

Le présent livre indique donc quelles sont les législations nationales qui transposent cette directive et quelles durées de conservation elles imposent.

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

2 | ZOOM
Ce que vous devez savoir sur la loi contre le terrorisme & autres dispositions légales en 5 points

	Loi contre le terrorisme & autres dispositions légales	Loi HADOPI
L'opérateur de communications électroniques est tenu de conserver…	∘ 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 (Décret n°2006-358 du 24 mars 2006, article R. 10-13 du CPCE)	
L'opérateur de communications électroniques ne doit pas conserver…	*« le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications »* (Article L. 34-I-V du CPCE)	
Les sanctions en cas de non respect de l'obligation de conservation des données sont…	Un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques et 375.000 euros pour les personnes morales. (Article L. 39-3 du CPCE)	
La durée de conservation des données est…	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. (Le décret du 24 mars 2006 prévoit des durées de conservations variables en fonction des finalités).	
Des données à délivrer aux personnes habilitées à les recevoir sous peine de sanctions pénales…	Les données conservées par l'opérateur de communications électroniques ne peuvent être transmises qu'à des personnes habilitées parmi lesquelles : - 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 ∘ le juge d'instruction ou l'officier de police judiciaire par lui commis au cours de l'instruction ∘ les agents individuellement habilités des services de police et de gendarmerie, spécialisés dans la prévention des actes de terrorisme (Articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale ainsi que l'article L. 34-1-1 du CPCE) 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 ».*	La commission de protection des droits de la HADOPI peut demander à l'opérateur de communications électroniques de lui remettre : ∘ nom de famille, prénoms ; ∘ Adresse postale et adresses électroniques ; ∘ Coordonnées téléphoniques ; ∘ Adresse de l'installation téléphonique de l'abonné (Décret n° 2010-236 du 5 mars 2010 en son article 2) *« 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. (Article R. 331-38 du décret n° 2010-872 du 26 juillet 2010)

3 | Ne pas conserver certaines données de connexion : 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 [1].

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 ».
Un décret n°2011-219 du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, est venu préciser quelles sont les données mentionnées au II de l'article 6 de la LCEN.

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 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 aborderons d'abord 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.

Il convient de préciser que pour ce qui concerne la France, les opérateurs de communications offrant un accès à l'internet au public sont tenus, en tant que responsable de traitement, à une obligation de déclaration à la Commission Nationale de l'Informatique et des Libertés (CNIL), au motif que les données collectées sont susceptibles de porter atteinte à la vie privée ou aux libertés et ne profitent dès lors pas d'une exonération de déclaration.

Nous envisagerons ensuite la question de la transposition de la directive 2006/24/CE dans l'Union Européenne. Cette directive contraint chacun des Etats membres à adopter une loi obligeant les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication à conserver les données relatives aux communications pour une durée comprise entre 6 et 24 mois. Nous indiquerons notamment quelles sont les durées de conservation des données prévues dans chacun des Etats membres.

[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.

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

La loi n°2006-64 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.

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.

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.

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.

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°2006-64 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 | TRANSPOSITION DE LA DIRECTIVE 2006/24/CE ET DURÉES DE CONSERVATION DES DONNÉES IMPOSÉES PAR LES ETATS MEMBRES

Date de la réalisation de l'étude : Janvier 2013

Même si la France, par le biais du décret n°2006-358 du 24 mars 2006 relatif à la conservation des communications électroniques qui faisait suite à la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, n'a pas eu à transposer la directive au motif que son droit interne était d'ores et déjà conforme, les 26 autres pays de l'Union Européenne devaient y procéder.

La directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE définit les règles et les procédures de conservation des données personnelles ainsi que des registres d'appels téléphoniques que doivent respecter les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication.
Cette directive exige la conservation des données relatives au trafic générées par l'utilisation des services de communication électronique pendant une période allant de six mois à deux ans[2].

Elle prévoit que la durée maximale de conservation de ces données peut être prolongée par un État membre s'il est « confronté à des circonstances particulières justifiant une prolongation, pour une période limitée » et à la condition que cette prolongation soit notifiée à la Commission, laquelle peut, dans un délai de six mois suivant la notification, approuver ou rejeter la prolongation. Si la durée maximale peut être prolongée, aucune disposition ne prévoit la réduction de la durée de conservation en deçà de six mois.

[2] L'article 6 de la directive dispose que : *« Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication ».*

L'obligation de conservation s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

En vertu de l'article 5 de la directive, les catégories de données à conserver sont :

a) les données nécessaires pour retrouver et identifier la source d'une communication
b) les données nécessaires pour identifier la destination d'une communication
c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication
d) les données nécessaires pour déterminer le type de communication
e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel
f) les données nécessaires pour localiser le matériel de communication mobile

Cette directive devait impérativement être transposée avant le 15 septembre 2007 par les Etats membres de l'Union européenne.

Le tableau qui suit vise à faire apparaître la durée de conservation des données qu'imposent les pays de l'Union européenne qui avaient, comme la France, l'obligation de transposer la Directive.

Il fait état des pays dans lesquels il n'y a pas encore de transposition de la directive, mais aussi des cas où des décisions de justice ont déclaré inconstitutionnelles les lois votées par les parlements nationaux[3] qui transposent la directive.

Il est utile de préciser qu'une législation sur la conservation des données existe également dans des pays qui ne font pas partie de l'Union européenne, mais de l'Espace Economique Européen (EEE) parmi lesquels l'Islande, le Liechtenstein et la Norvège[4].

[3] République Tchèque et Allemagne.
[4] La loi islandaise est une loi sur les télécommunications 81/2003 telle que modifiée en avril 2005. Au Liechtenstein, il s'agit d'une loi sur les télécommunications de 2006. En Norvège, une loi a été votée le 5 avril 2011.

Pays	Textes de loi transposant la Directive	Durées de conservation des données fixée dans la législation nationale	Remarques
Allemagne	Loi de révision sur la surveillance du secteur des télécommunications et d'autres mesures d'enquête ainsi que sur la mise en œuvre de la directive 2006/24/CE Date de publication 31/12/2007 Entrée en vigueur : 01/01/2008	12 mois à compter de la date de la communication. Dans l'attente d'une nouvelle loi transposant la directive 2006/24/CE fixant éventuellement une durée différente.	La Cour constitutionnelle fédérale allemande a déclaré inconstitutionnelle certaines dispositions de la loi allemande transposant la directive par un arrêt en date du 2 Mars 2010 le 27 octobre 2011, la Commission a formellement invité l'Allemagne à prendre, dans un délai de deux mois, des mesures permettant d'assurer le plein respect des règles de l'UE relatives à la conservation des données Le 26 mars 2012, la Commission a averti l'Allemagne qu'elle saisira la Cour de Justice de l'Union Européenne (ci-après CJUE) afin que cette dernière prononce des amendes à son égard Compte tenu du fait que les autorités allemandes n'ont pas faire savoir comment ni quand elles entendaient adopter une nouvelle législation transposant pleinement la directive 2006/24/CE, la Commission a décidé de porter l'affaire devant la CJUE La Commission a notamment proposé à la Cour d'infliger une astreinte de 315 036,56 euros par jour de retard jusqu'à ce que l'Allemagne se mette en conformité avec le droit de l'Union.
Autriche	Loi fédérale modifiant la loi sur les télécommunications de 2003 Date de publication : 18/05/2011 Entrée en vigueur : 19/05/2011	6 mois à compter de la date de la communication	

Belgique	Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Arrêté royal du 9 janvier 2003 portant exécution des articles 46 bis, § 2, alinéa 1er, 88 bis, § 2, alinéas 1er et 3, et 90 quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109 ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques	12 à 36 mois pour les services téléphoniques accessibles au public. Il n'existe pas encore de transposition pour les services internet	La Belgique est donc toujours dans l'attente d'une loi transposant la directive 2006/24/CE dans son intégralité. Un avant projet de loi sur la conservation des données du 27 août 2009 prévoit une durée de conservation de 24 mois. Certains acteurs interrogés préconisent d'abaisser la durée de conservation des données à 12 mois
Bulgarie	Loi sur les communications électroniques Date de publication: 02/03/2010 Entrée en vigueur: 10/05/2010 Ordonnance N°40 du 7 Janvier 2008 propres à certaines catégories de données et la façon dont elles sont stockés et mises à disposition par les entreprises fournissant des réseaux de communications électroniques et / ou des services dans l'intérêt de la sécurité nationale et de la détection de la criminalité Date de publication: 29/01/2008 Entrée en vigueur: 01/02/2008	12 mois à compter de la date de la communication. Les données auxquelles l'accès a été accordé peuvent être conservées six mois de plus sur demande	Une action relative à la conservation des données a été introduite devant la Cour administrative suprême de Bulgarie (arrêt n°13627 du 11 décembre 2008) Cela a entrainé une révision de la loi de transposition
Chypre	La loi sur la conservation des données de télécommunications pour les crimes graves. Date de publication 31/12/2007 Entrée en vigueur : 31/12/2007	6 mois à compter de la date de la communication	Plusieurs affaires relatives à la conservation des données ont été portées devant la Cour constitutionnelle chypriote (affaires n°65/2009, 78/2009 et 15.2010-22.2010 du 1er février 2011). La Cour a jugé inconstitutionnelles les ordonnances des tribunaux rendues en vertu de la loi de transposition La loi de transposition reste néanmoins valable

Danemark	Première, deuxième et troisième ordonnance sur les fournisseurs de réseaux de communications électroniques et de services de communications électroniques d'enregistrement et le stockage de l'information sur le trafic Date de publication : 13/10/2006 Entrée une vigueur: 15/09/2007	12 mois à compter de la date de la communication	
Espagne	Loi n°25/2007 de conservation des données sur les communications électroniques et des réseaux de communications publics Date de publication : 19/10/2007 Entrée en vigueur: 08/11/2007		Une autorité compétente peut, après consultation des opérateurs de télécommunications électroniques, réduire cette durée de conservation à 6 mois ou au contraire l'augmenter à 24 mois pour certaines données ou catégories de données
Estonie	Loi sur les communications électroniques et la santé publique Date de publication et d'entrée en vigueur : 07/12/2007	12 mois à compter de la date de la communication	
Finlande	Loi d'obligation d'identification et de stockage des données / Loi sur la vie privée dans les communications électroniques Entrée en vigueur : 05/06/2008	12 mois à compter de la date de la communication	La Finlande n'impose pas aux petits opérateurs l'obligation de conserver les données au motif que les coûts que cela représente tant pour le fournisseur que pour l'État dépasseraient les bénéfices pour les services répressifs et la justice pénale
Grèce	Loi de conservation des données générées ou traitées en collaboration avec les réseaux publics de communications, l'utilisation de systèmes de surveillance, de réception ou d'enregistrement audio ou vidéo dans les lieux publics et dispositions connexes Date de publication : 21/02/2011	12 mois à compter de la date de la communication	

Hongrie	Loi de 2003 sur les communications électroniques Date de publication : 13/12/2003 Loi de 2007 modifiant la loi sur les communications électroniques	6 mois pour les appels téléphoniques infructueux et 12 mois pour toutes les autres données	Une action a été introduite le 2 juin 2008 par l'union hongroise des libertés civiles devant la Cour constitutionnelle hongroise. Elle est actuellement pendante
Italie	Loi de mise en œuvre de la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou réseaux de communications publics et modifiant la directive 2002/58/CE Date de publication : 18/06/2008	12 mois à compter de la date de la communication	
Irlande	Loi sur la conservation des données de communications de 2011 Date de publication: 28/01/2011	24 mois pour les données de téléphonie fixe et mobile 12 mois pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet	Le 11 juin 2012, la High Court of Ireland a adressé à la Cour de Justice de l'Union Européenne, une demande de décision préjudicielle portant sur la directive 2006/24/CE enregistrée sous le numéro d'affaire C-293/12. Aucune réponse n'a encore été formulée par la CJUE.
Lettonie	Modifications de la Loi sur les communications électroniques du 17/11/2004 Date de publication: 24/05/2007 Entrée en vigueur: 07/06/2007 Procédures obligeant les opérateurs de communication électronique à recueillir et à conserver des informations statistiques sur les données et à les délivrer sur demande aux autorités d'enquête avant le procès, aux exploitants d'urgence, aux autorités de sécurité nationale et au ministère public selon ordonnances du tribunal Date de publication: 07/12/2007 Entrée en vigueur: 08/12/2007	18 mois à compter de la date de la communication	

Lituanie	Loi lituanienne sur les communications électroniques Date de publication: 29/11/2008 Entrée en vigueur: 15/03/2009	6 mois à compter de la date de la communication	
Luxembourg	Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. Date de publication: 29/07/2010 Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle Date de publication: 29/07/2010	6 mois à compter de la date de la communication	
Malte	Loi modificative sur la protection des données de 2008 (LN. 198) Date de publication 29/08/2008 Loi sur les communications électroniques régulation) (LN. 198) (CAP 399) Date de publication : 29/08/2008	12 mois pour toutes les données relatives à la téléphonie fixe, mobile et par l'internet 6 mois pour toutes les données relatives à l'accès à l'internet et au courrier électronique par l'internet	
Pays-Bas	Loi du 18 Juillet 2009 modifiant la loi sur les télécommunications et les infractions économiques en relation avec la mise en œuvre de la directive 2006/24/CE du Parlement européen et du Conseil de l'Union européenne sur la rétention de données traitées dans le cadre avec la fourniture de services de communications électroniques et modifiant la directive 2002/58/CE (Loi sur la conservation des données de télécommunications)	12 mois à compter de la date de la communication	
Pologne	La réglementation du 28 Décembre 2009 du ministère des infrastructures concernant une liste complète de données et l'obligation de conservation à laquelle sont tenus les exploitants de réseaux publics de télécommunications ou de services de télécommunications accessibles au public. Loi du 24 avril 2009 modifiant la Loi sur les télécommunications du 16 juillet 2004 Décret du 22 Mars 2010 sur la façon de transmettre et de partager des données en cas de faillite d'un opérateur de réseau public de télécommunications ou un fournisseur de services de télécommunications accessibles au public	24 mois à compter de la date de la communication	

Portugal	Transposition en droit national de la directive 2006/24/CE du Parlement européen et du Conseil du 15 Mars, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques services ou des réseaux publics de communications Date de publication: 17/07/2008	12 mois à compter de la date de la communication	
République Tchèque	Loi n ° 247/2008 Coll. Modifiant la loi n° 127/2005 Coll. Communications électroniques et modifiant certaines lois connexes Date de publication: 04/07/2008 Décret n ° 485/2005 Coll. La mesure du trafic et des temps de rétention des données de localisation et leur transmission aux organismes habilités à les utiliser Date de publication: 15/12/2005	De 6 à 12 mois à compter de la date de la communication. Déclarée inconstitutionnelle, elle devra faire l'objet d'une nouvelle transposition	Un arrêt de la Cour constitutionnelle tchèque du 22 mars 2011 a déclaré inconstitutionnelles la loi n°127/2005 et le décret n°485/2005. La République Tchèque examine actuellement comment procéder à une nouvelle transposition de la directive.
Roumanie	Loi sur la conservation de données générées ou traitées par les fournisseurs de services de communications électroniques ou réseaux de communications publics modifiant la loi n°506/2004 sur le traitement des données personnelles et la vie privée dans le secteur des communications électroniques (loi n° 298/2008) Date de publication : 21/11/2008 Loi n°82/2012 du 22 mai 2012 relative à la conservation des données générées ou traitées par les fournisseurs de réseaux de communications électroniques et par les services de communications électroniques destinés au public Date d'entrée en vigueur : 18 juin 2012	6 mois à compter de la date de la communication	Le 8 octobre 2009, la Cour constitutionnelle roumaine a jugé inconstitutionnelle la loi n° 298/2008 de transposition de la directive. le 27 octobre 2011, la Commission Européenne a formellement invité la Roumanie à prendre, dans un délai de deux mois, des mesures permettant d'assurer le plein respect des règles de l'UE relatives à la conservation des données Le 22 mai 2012, la Chambre des députés du Parlement roumain a adopté à une large majorité la loi relative à la conservation des données générées ou traitées par les fournisseurs de réseaux de communications électroniques et par les services de communications électroniques destinés au public
Royaume-Uni	Règlement sur la conservation des données de 2007 Entrée en vigueur: 01/10/2007 Règlement sur la conservation des données de 2009 Entrée en vigueur: 06/04/2009	12 mois à compter de la date de la communication	Le Royaume-Uni n'impose pas aux petits opérateurs l'obligation de conserver les données au motif que les coûts que cela représente tant pour le fournisseur que pour l'État dépasseraient les bénéfices pour les services répressifs et la justice pénale.

Slovaquie	Loi n ° 654/2007 modifiant et complétant la loi n °610/2003 sur les communications électroniques	12 mois pour les données de téléphonie fixe et mobile, 6 mois pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet	
Slovénie	Règles relatives à la méthode de transmission des données de trafic détenues par services de la téléphonie mobile et les réseaux fixes de communications électroniques Date de publication: 14/12/2009 Entrée en vigueur: 13/01/2010 Loi modifiant la loi sur les communications électroniques Date de publication: 12/12/2006	8 mois pour les données relatives à l'internet. 14 mois pour les données de téléphonie	
Suède	Loi 2012/278 concernant la collecte des données sur les communications électroniques en application de la loi intelligence. Date de publication : 21 mars 2012 Date d'entrée en vigueur : 1er mai 2012	6 mois à compter de la date de la communication	La Suède a été déclarée coupable de manquement à l'obligation qui lui incombe en vertu de l'UE par la Cour de justice (C-185/09). En avril 2011, la Commission a intenté un second recours contre la Suède devant la Cour pour inexécution de l'arrêt rendu dans l'affaire C-185/09. La Suède s'exposait à une sanction financière en vertu de l'article 260 du traité sur le fonctionnement de l'Union Européenne à la suite de la décision de son parlement de retarder d'un an l'adoption de la loi de transposition. Le Parlement suédois a voté le 21 mars 2012 la Loi 2012/278 concernant la collecte des données sur les communications électroniques en application de la loi intelligence. Cette loi transpose la directive 2006/24/CE. Cela a abouti à ce que le 31 mai 2012, la Commission abandonne partiellement la procédure de sanctions visant la Suède. Conformément à sa pratique dans le cas où un Etat membre transpose une directive à un moment où une procédure de sanction a déjà atteint le stade d'une seconde saisine de la Cour de justice, la Commission a, en effet, retiré la demande d'astreinte tout en maintenant la demande visant à ce que la Suède soit condamnée à payer une somme forfaitaire.

CONCLUSION

Nous venons de voir ce qu'ont décidé les Etats membres concernant la durée de l'obligation de conservation des données relatives au trafic et des données de localisation qu'ils étaient tenus d'imposer aux opérateurs de communications électroniques opérant sur leur territoire.

Même si certains des Etats membres n'ont pas encore transposé la directive, ou ont vu leurs juridictions internes censurer la loi qui était venue la transposer, la conservation des données a toujours eu pour vocation d'aider les systèmes de justice pénale et les services répressifs de l'Union européenne.

La directive prévoit, en effet, que les données doivent être conservées à des fins de recherche, de détection et de poursuites graves.

L'opérateur de communication électronique qui souhaite fournir un accès à l'Internet au public dans l'un des 27 pays membres de l'Union européenne et plus particulièrement dans ceux qui, à l'heure actuelle, ont transposé la directive 2006/24/CE, devra donc s'assurer de **disposer des outils techniques permettant une collecte des données relatives au trafic et des données de localisation des internautes** répondant précisément aux préconisations de la loi transposant la directive en droit interne et ne pas oublier que ces données ne devront être communiquées qu'à un nombre restreint d'autorités habilitées à se les faire délivrer.

Pour plus d'informations : http://eur-lex.europa.eu

5 | LA CNIL

L'opérateur de communication électronique : un responsable de traitements sur lequel pèsent également des obligations liées au caractère personnel des données qu'il collecte.

Dans l'hypothèse où l'opérateur de communication électronique recueille des données présentant des risques particuliers d'atteinte aux droits et aux libertés, celui-ci devra veiller à obtenir une autorisation préalable de la Commission Nationale Informatique et Libertés.

Le non-accomplissement de ces formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende conformément à l'article 226-16 du Code pénal.

Tout responsable de traitement informatique de données personnelles doit également mettre en place des mesures de sécurité physiques, logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement.

Le non-respect de cette obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende est sanctionné par l'article 226-17 du Code pénal.
Il devra également veiller à ce que seules les personnes autorisées puissent accéder aux données personnelles contenues dans les fichiers collectés (destinataires explicitement désignés et tiers autorisés – police, services des impôts).

Le responsable du fichier devra aussi s'assurer qu'il permet aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits de modification, de suppression et de retrait dudit fichier.

Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 euros par infraction constatée et 3 000 euros en cas de récidive (Article 131-13 du Code pénal, Décret n°2005-1309 du 20 octobre 2005).

Le responsable du fichier devra respecter le principe dit de la finalité du traitement qui veut que les informations exploitées dans un fichier soient cohérentes par rapport à son objectif.

Les informations collectées ne pourront pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.
Le non respect de cette règle est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-21 du Code pénal).

6 | LES PRINCIPES DE LA CHARTE INTERNET

Qu'est-ce qu'une charte Internet ?

La **charte Internet** définit les conditions générales d'utilisation des accès internet et des réseaux au sein d'une entreprise.
On y recense les droits, les responsabilités et les obligations des salariés. Ce document permet ainsi d'éviter tout usage abusif des outils informatiques et peut être utilisé en tant que référence en cas de conflit.

La charte : une obligation ?

Elle est obligatoire dans le seul cas où l'entreprise collecte des données personnelles sur ses salariés : durée de connexion, archivage de messagerie…
Chacun des salariés de l'entreprise doit être informé de la mise en place d'un outil de filtrage par le biais d'un document rédigé.
La CNIL (Commission Nationale Informatique et Libertés) recommande l'adoption d'une charte Internet ayant pour objectif de «sensibiliser les salariés ou les agents publics aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration».

L'intérêt de mettre en place une charte ?

LIMITER SES RESPONSABILITÉS

- NÉGLIGENCE FAUTIVE

Article 1383 du Code Civil :
« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »
Cet article met en avant la responsabilité de ne pas avoir mis en place les moyens nécessaires pour éviter toute déviance. Il s'agira de responsabilité pour « négligence fautive ».

- RESPONSABILITÉ CIVILE

Article 1384 du Code Civil :
« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre (…) les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés »

- RESPONSABILITÉ PÉNALE

Article 121-1 du Code Civil :
« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement (…) des infractions commises, pour leur compte, par les organes dirigeants ou représentants »
La responsabilité pénale de l'entreprise et de ses dirigeants peut être engagée dans le cas où l'infraction sert les intérêts de l'entreprise.

7 | UNE RÉPONSE ADAPTÉE : NOTRE SOLUTION

Les solutions UCOPIA répondent aux besoins des établissements souhaitant s'équiper d'une connexion Internet sécurisée (Wi-Fi en libre accès, connexion invités…) dans l'objectif 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,**
- **ou encore des administrations,**

permettent aux utilisateurs de se connecter de manière sécurisée au réseau et d'utiliser les applications métier, Internet ou bien la téléphonie de façon simple et sûre.

Les performances techniques, la simplicité de mise en service et le respect rigoureux de la réglementation font de ces solutions le produit de référence actuel.

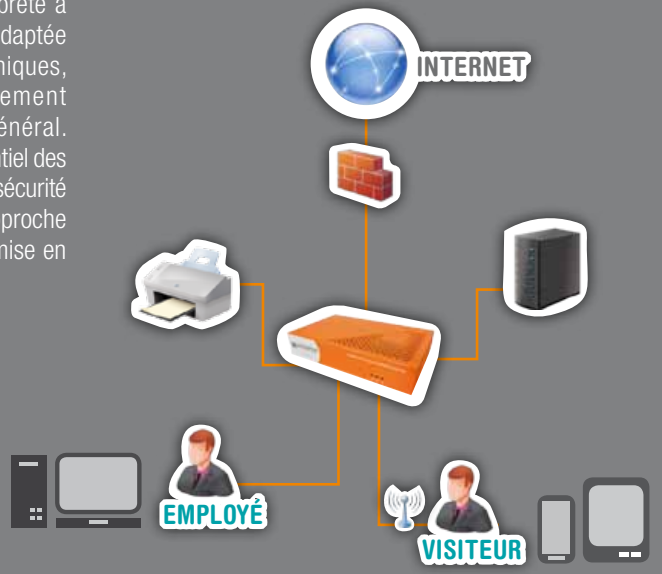
L'offre UCOPIA se compose en deux gammes : **la gamme Express et la gamme Advance.**

UCOPIA est le seul produit combinant :

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

UCOPIA EXPRESS

La gamme **UCOPIA Express** se présente sous la forme d'une solution prête à l'emploi et est parfaitement adaptée aux besoins des hôtels, cliniques, établissements d'enseignement secondaires et PME en général. UCOPIA Express propose l'essentiel des fonctions UCOPIA en termes de sécurité et de nomadisme dans une approche privilégiant la simplicité de la mise en œuvre et de l'administration.



LES FONCTIONNALITÉS CLEFS

VLAN entrée / sortie

Connexions sans fil / filaire

Portail captif
- Entièrement personnalisable
- Authentification sécurisée par HTTPS
- Annuaire LDAP interne
- Couplage annuaire LDAP d'entreprise
- Compatibilité Shibboleth
- Multi-portails / multi modes

Authentification forte 802.1x (PEAP, TTLS)

Contrôle d'accès par profil utilisateur
- QoS
- Plages horaires, crédit temps

Filtrage d'URLs

Provisionnement de comptes
- Délégation (accueil visiteur)
- Auto-provisionnement par
  - Formulaire web
  - SMS
  - Mail
- Auto-enregistrement sécurisé
- One click button
- Forfaits par paiement en ligne
- Applications mobiles

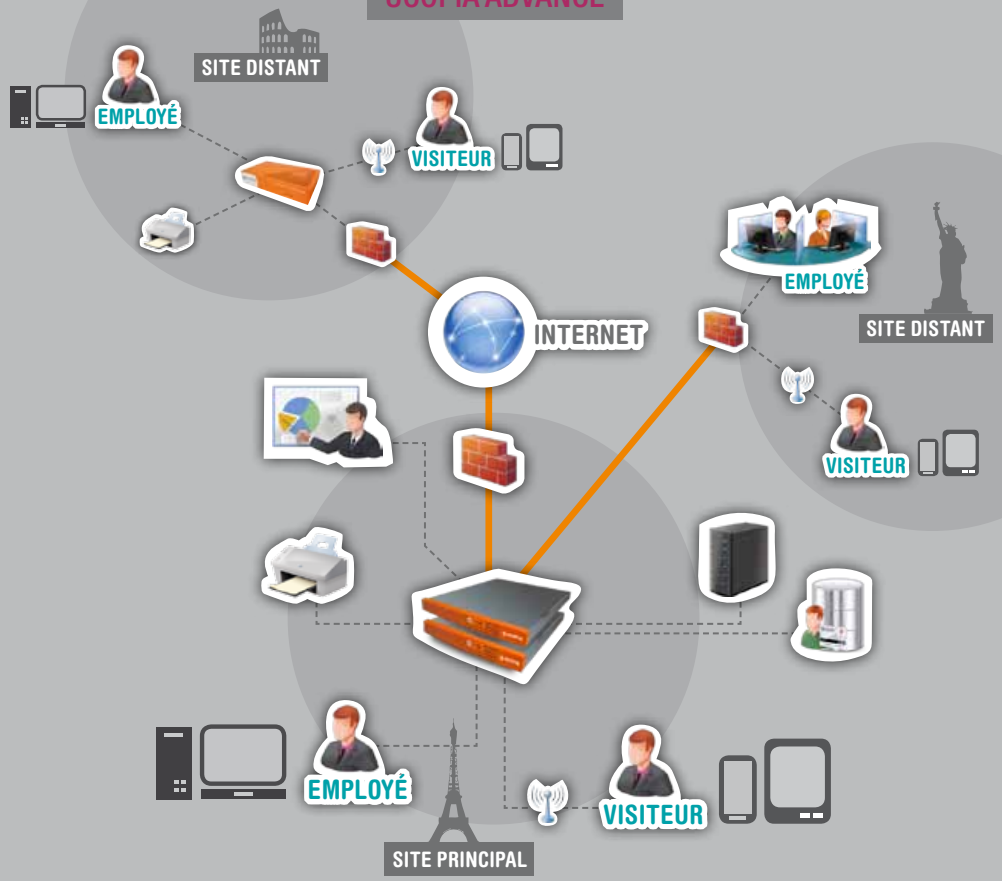
Zéro configuration IP / Proxy web /impression

Journal des sessions utilisateurs, activités, URLs

SNMP, Syslog, CLI

Reporting d'utilisation

UCOPIA ADVANCE



La gamme **UCOPIA Advance** physique et virtualisée, est une solution qui propose l'ensemble des fonctionnalités UCOPIA et qui est destinée aux moyens et grands projets des entreprises, des campus et des administrations. UCOPIA Advance permet de répondre aux besoins des environnements multi sites et propose toutes les fonctions d'intégration avec le LAN de l'entreprise. UCOPIA Advance peut être redondée et fonctionne également en répartition de charge.

LES FONCTIONNALITÉS CLEFS

Toutes les fonctionnalités Express plus :

- Intégration forte avec le réseau (annuaire LDAP en cascade, RADIUS proxy…)
- Authentification forte par certificat (802.1x EAP/TLS)
- Profils adaptables
- Redondance / Répartition de charge
- Architecture multi contrôleurs

IMPLÉMENTATION RÉSEAU

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, les solutions UCOPIA peuvent gérer de 5 à plus de 100 000 utilisateurs simultanés et s'installent très simplement dans l'infrastructure réseau.

La solution UCOPIA se place entre un réseau d'accès filaire (Ethernet, DSLAM, CPL) ou sans-fil (Wi-Fi) et le LAN de l'organisation. UCOPIA est compatible avec tous les fournisseurs d' équipements de Wi-Fi (CISCO, Ruckus etc)

LES PRINCIPAUX AVANTAGES DE LA SOLUTION

- Une gamme complète et évolutive (plusieurs milliers de connexions simultanées)
- La sécurité combinant l'authentification, le contrôle d'accès par profil et la traçabilité des connexions : UCOPIA est le seul produit certifié par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information)
- Des coûts d'exploitation réduits de 90%
- Un portail captif totalement personnalisable
- La simplicité de mise en œuvre et d'administration
- Un retour sur investissement < 6 mois
- Filtrage d'URLs
- Une gestion précise des indicateurs de performance
- L'accès zéro configuration (pas besoin d'assistance technique)
- Le confort d'utilisation (multi portails d'accueil)
- Une gestion des accès adaptée à toutes les situations
  - Par auto-enregistrement avec ou sans 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
  - Grâce à un portail «One click Button»

8 | NOS PRINCIPAUX DÉPLOIEMENTS MÉDIATIQUES EN 2012

PHILIPS

PHILIPS

sense and simplicity

Philips propose, à son siège de Suresnes, un accès internet pour ses visiteurs, et maîtrise également son BYOD, grâce à UCOPIA. Les visiteurs sont enregistrés de façon simple à l'accueil du site via l'interface de délégation UCOPIA, et les employés peuvent authentifier leurs appareils personnels avec leurs identifiants Active Directory Philips.

NORFOLK & NORWICH HOSPITAL

Norfolk and Norwich University Hospitals NHS
NHS Foundation Trust

Le CHU de Norwich (Comté de Norfolk en Angleterre) sécurise les accès internet sans fil de ses visiteurs et patients, ainsi que le BYOD du personnel soignant. Plus de 1000 connexions simultanées quotidiennes sont enregistrées sur un cluster de contrôleurs UCOPIA en redondance.

HÔTEL PRÉSIDENT WILSON GENÈVE

Cet hôtel prestigieux est équipé d'une solution UCOPIA Express 250 qui propose 3 types de connexions réseau :

- Pour les clients du SPA
- Pour les utilisateurs des salles de réunions
- Pour les clients de l'hôtel

L'hôtelier utilise pour connecter les utilisateurs un identifiant unique. Une évolution du système prévoit d'utiliser la solution d'auto-enregistrement SMS pour la gestion simplifiée des accès utilisateurs.

IFREMER

Ifremer

L'Institut Français de Recherche pour l'Exploitation de la Mer (IFREMER) a choisi de faire confiance aux solutions UCOPIA pour sécuriser ses connexions internet dans ses salles de réunion et dans les ateliers. L'institut utilise l'authentification de ses connexions par le mécanisme Shibboleth.

STADE DE FRANCE

Le Stade de France bénéficie d'un accès internet totalement sécurisé permettant la connexion des tablettes et Smartphones des journalistes et des VIPs.

9 | À PROPOS D'UCOPIA COMMUNICATIONS

UCOPIA a équipé plus de :

1900 hôtels

800 établissements de santé

1500 PME et grands comptes

1250 établissements scolaires

1250 établissements publics

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 **7500 clients** dans tous les secteurs
- Un réseau de plus de **150 partenaires européens**
- Plus de **180 millions de connexions** en 2012 sur les solutions UCOPIA
- **50% de croissance annuelle** sur les six dernières années
- Un siège social à **Paris**, des bureaux à **Munich**, **Milan** et **Londres**

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

HÔTELS

Hôtel Bristol Genève

starwood Hotels and Resorts

InterContinental Hotels & Resorts

Ritz Paris

ÉDUCATION

HEC Paris

INSEAD

American School of Paris

cnrs

SANTÉ

Hôpital Erasme ULB

Clinique de La Source Lausanne

West Suffolk Hospital NHS Trust

Barts Health NHS Trust

Norfolk Community Health and Care NHS Trust

ENTREPRISES

REHAU Unlimited Polymer Solutions

Peugeot

Carrefour

L'Oréal

Danone

COLLECTIVITÉS ET HOTSPOT

palexpo

Stade de France

European Parliament

GL events

Aéroport de Bordeaux

NATO OTAN

www.ucopia.com

UCOPIA Communications
201, Avenue Pierre Brossolette 92120 - MONTROUGE
Tél. : + 33 (0) 1 40 92 73 90 - Fax : + 33 (0) 1 40 92 73 99
Email : contactus@ucopia.com

CRÉDITS PHOTO : FOTOLIA - CRÉATION GRAPHIQUE : CLAIRE TAGLIAFERRI - CONTACT@CLAIRE-DA.COM - 06 80 14 10 00