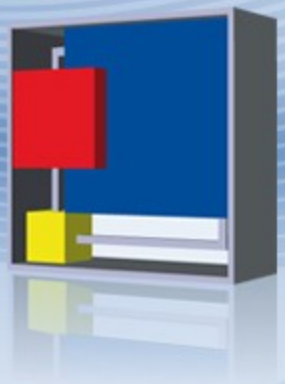
Bonnes pratiques juridiques
Administrateur Systèmes & Réseaux



ALAIN BENSOUSSAN
LE DROIT DES TECHNOLOGIES AVANCÉES

Eric Barbry
Avocat
Directeur du pôle « droit du numérique »

PLAN

Thème 1 - Actualité du droit des SI

Thème 2 - Bonnes pratiques ASR

ACTUALITE DU DROIT DES SYSTEMES D'INFORMATION

1. Zoom arrière…

1. Aspect réglementaire
2. Aspect jurisprudence

Le socle de base… connu de tous ☺

Art 1383 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 »

1384 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 »

121-2 Code pénal

« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement (….) des infractions commises, pour leur compte, par les organes dirigeants ou représentants »

Le droit à la protection – Art. 323-1 Code pénal

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende ».

Le droit à la protection – Art. 323-2 Code pénal

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

Le droit à la protection – Art. 323-3 Code pénal

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende »

Le droit à la protection – Art 323.3.1 Code pénal

« Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Renforcement du droit de sécuriser son SI
Disposition générale

« La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives »

(Article 1er de la loi n°95-73 du 24 janvier 1995 d'orientation et de programmation relative à la sécurité modifiée par la LSI (18 mars 2003) et par la loi relative à la lutte contre le terrorisme (23 janvier 2006)

Renforcement du droit de sécuriser son SI – Dispositions spécifiques

- De la sécurité dans les lois générales
  - Ex : Informatique et libertés – Hadopi
- Des obligations sectorielles
  - Ex : Secret défense
- Des obligations par acteurs
  - Ex : hébergement de données de santé – Opérateur infrastructure vitale
- Des obligations par acteurs ou services
  - Ex : dématérialisation – commande publique

Le schéma de Laurette…

Zoom Informatique et libertés - Sécurité

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité
des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'Informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8. » - Art. 34 I&L

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. » – Art 35 I&L

Une conséquence majeure…

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »

Article 226-17 du code pénal

Obligation de sécuriser : la jurisprudence

- IBM/Flammarion
  - Le SI est un « produit dangereux »
- Tati/Kitetoa
  - Pour prétendre être victime d'une intrusion, encore faut-il démontrer avoir sécurisé son SI et marqué ses données
- Escota/lucent
  - Responsabilité de l'employeur du fait de son salarié

L’obligation de contrôler

- Code civil
  - article 1384 : responsabilité de l’employeur vis-à-vis de son salarié
- Code pénal
  - Nul n’est responsable que de son propre fait
    - Mais la responsabilité pénale de l’entreprise et des dirigeants est toujours possible

(re)Naissance de la vie privée résiduelle

- Une réalité de longue date
- Ré-activité par la jurisprudence
- Une pratique logique
- Une pratique admise par tous
  - Cnil et Forum des droits sur Internet

Le principe de base

Arrêt Nikon du 2 oct. 2001

« L'employeur ne peut, sans violation du secret des correspondances (liberté fondamentale), prendre connaissance des messages personnels et ceci même au cas où il aurait interdit l'usage non professionnel de l'ordinateur »

Présomption « professionnel »

« L'employeur ne peut, sans violation du secret des correspondances (liberté fondamentale), prendre connaissance des messages personnels et ceci même au cas où il aurait interdit l'usage non professionnel de l'ordinateur »

Cass. soc. 2 oct. 2001 - Arrêt Nikon

« Les connexions établies par un salarié sur des sites Internet »

- Cass. soc. 9 juill. 2008

« Les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur »

- Cass. soc. 18 oct. 2006 Techni-Soft

« Les documents détenus par le salarié dans le bureau de l'entreprise mis à sa disposition »

- Cass. soc. 18 oct. 2006 Entreprise Jalma

Les limites de la vie privée résiduelle

- La vie privée résiduelle est limitée
  - Cour d'appel de Rennes
- L'adresse mèl est « professionnelle »
  - CAA Paris, Ministère de l'éducation nationale
- La vie privée ne peut nuire à la continuité du service
  - Code d'accès
- Risque ou évènement particulier
  - Arrêt du 17 mai 2005 « Sauf risque ou évènement particulier » l'employeur ne peut « ouvrir les fichiers identifiés par le salarié comme personnels » « qu'en présence de ce dernier ou celui-ci dûment appelé »

Vie privée résiduelle – En pratique

- Nommage des dossiers informatiques et de mèl
  - « privé »
    - Pas de « choix » pour l'utilisateur
- Poste en libre service
- Webmail
- Double adresse

2. Evolution réglementaire 2010

1. 2010, un millésime
2. Revue de détail

2010 UN MILLESIME…

HADOPI

SECRET DEFENSE

RGS

INFORMATIQUE ET LIBERTES

JEUX D'ARGENT

L'HADOPI un vrai nouveau risque

Article L336-3 du CPI

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1.

Article L335-7-1 du CPI

Pour les contraventions de la cinquième classe prévues par le présent code, lorsque le règlement le prévoit, la peine complémentaire définie à l'article L. 335-7 peut être prononcée selon les mêmes modalités, en cas de **négligence caractérisée**, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel la commission de protection des droits, en application de l'article L. 331-25, a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet.
La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un an après la présentation de la recommandation mentionnée à l'alinéa précédent.

Dans ce cas, la durée maximale de la suspension est d'un mois.

HADOPI… La mise en œuvre

Impact

- Obligation légale
- Nouvelle sanction civile
  - Sur l'abonné …
- Sanction pénale possible
  - Sur l'abonné
- Abonné = employeur

Plan d'actions

1. Outils (filtrage)
2. Monitoring des outils
3. Information
4. Déclaration
5. Réaction aux notifications »

Pourquoi j'aime l'Hadopi

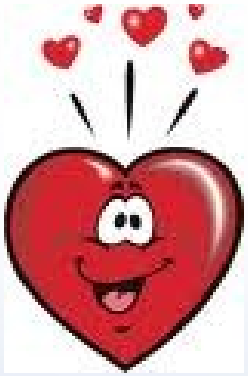
Une loi nécessaire

Une loi équilibrée

Une loi juste

Une loi efficace

Une loi de la dernière chance



Mort industrie culturelle

Sensibilisation/promotion

L'abonné a un rôle central

Un homme averti…

Jusqu'ici toutes les autres solutions ont échoué

Pourquoi vous allez aimer l'Hadopi…

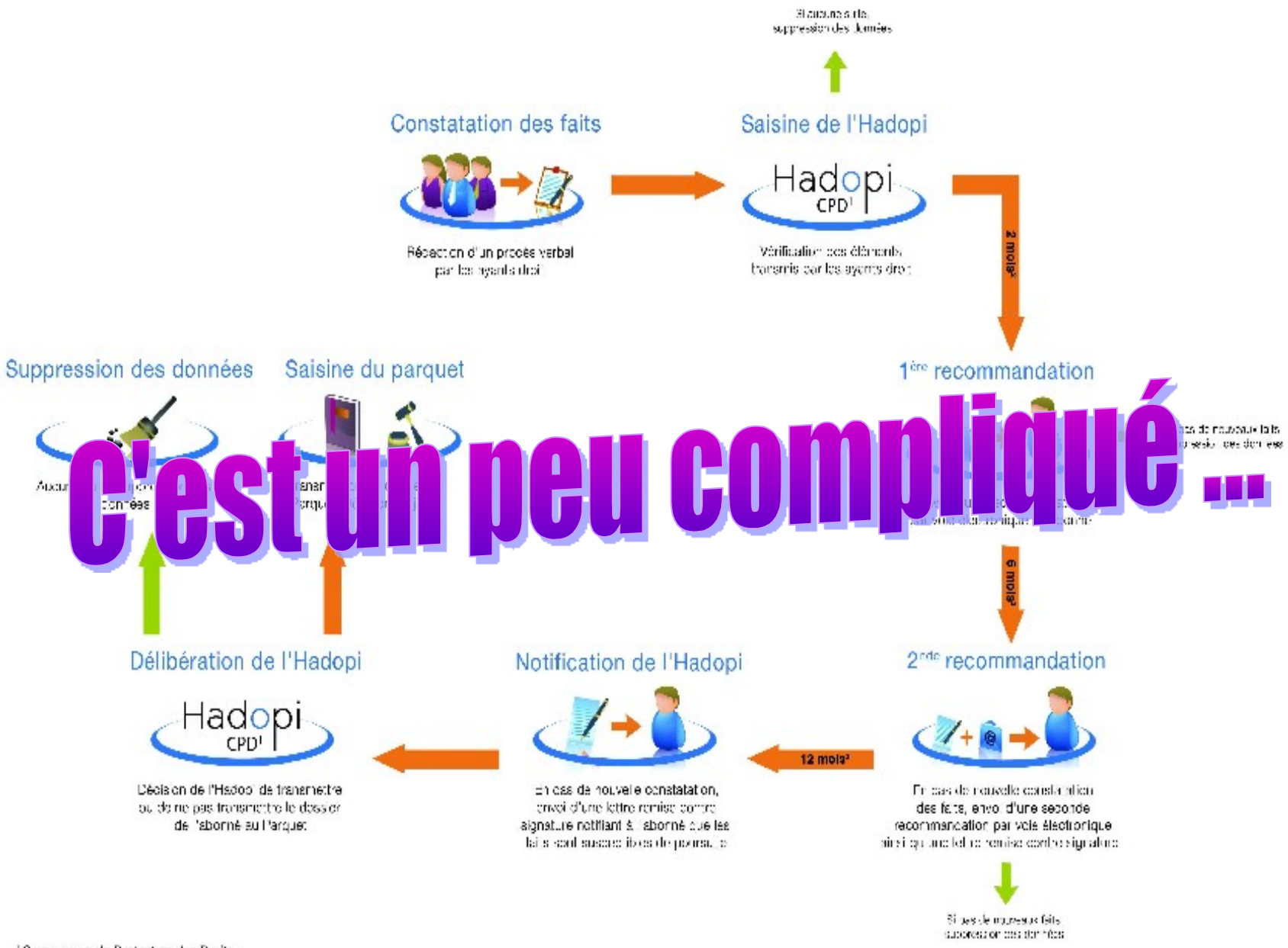
- **deBILL** – UK – Digital Economy Bill
  - Limitation bande passante puis suspension

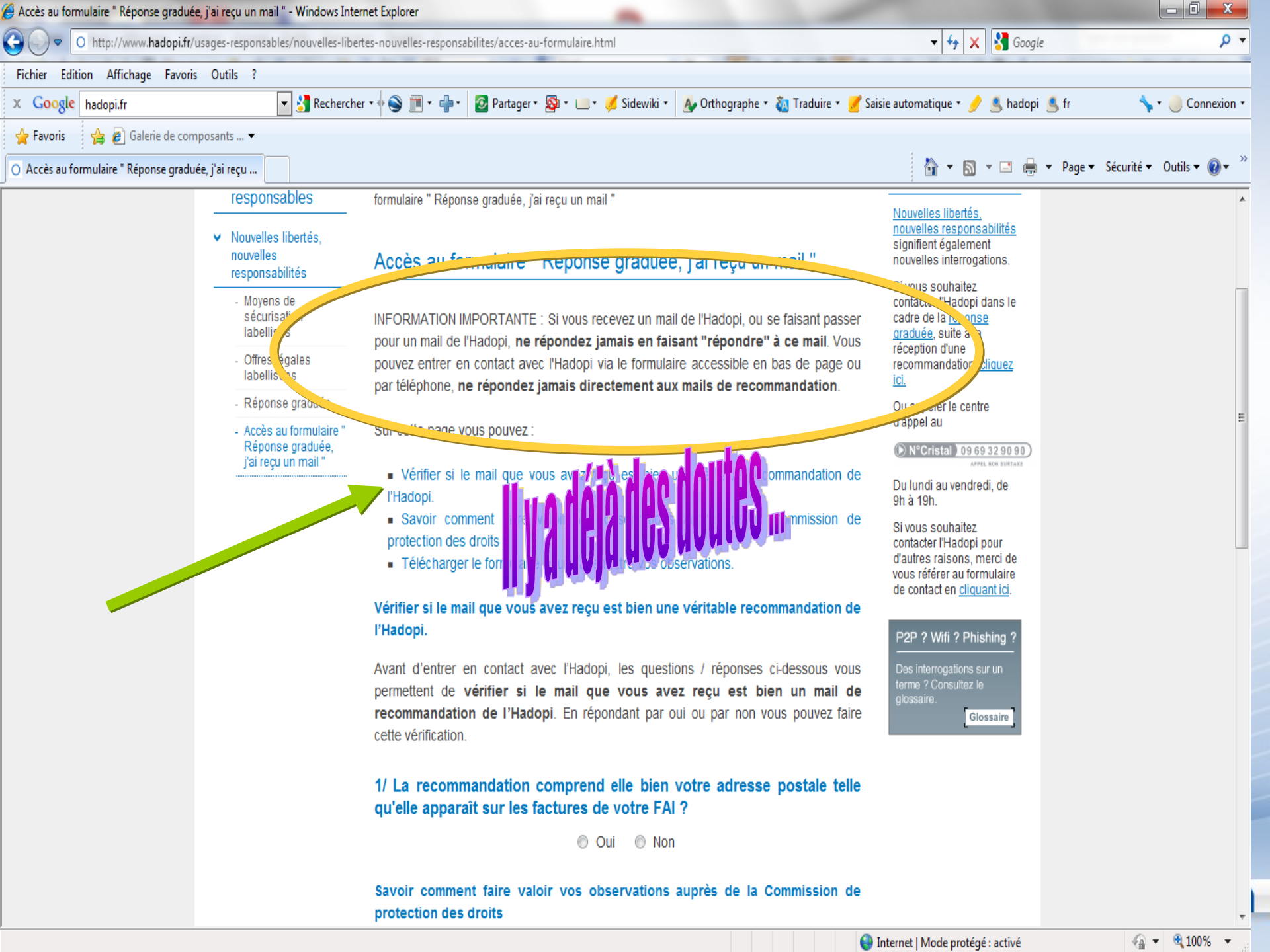
- Proposition :
  - Belgique - Loi favorisant **la protection de la création culturelle sur Internet** – Belgique – Proposition Monfils
  - Espagne – Loi sur « blocage a la source »

- Sytème Autre (Irlande) – Accord 2009 Fédé producteur de musique et 1er FAI du Pays – Avertissement + blocage à la source

- **IPRED2** – Union européenne - Second Intellectual Property Rights Enforcement Directive [*directive relative aux mesures pénales visant à assurer le respect des droits de propriété intellectuelle]*
  - *Exit la protection du Paquet télécom (amendement 138)*

- **ACTA** – Anti-Countefeiting Trade Agreement


Constatation des faits
Saisine de l'Hadopi
Hadopi
CPD¹
2 mois²
1ère recommandation
6 mois³
2nde recommandation
12 mois³
Notification de l'Hadopi
Délibération de l'Hadopi
Hadopi
CPD¹
Saisine du parquet
Suppression des données
C'est un peu compliqué ...
¹ Commission de Protection des Droits
² Délai maximum
³ Délai maximum entre l'envoi de la recommandation et les nouveaux faits


Accès au formulaire " Réponse graduée, j'ai reçu un mail " - Windows Internet Explorer
http://www.hadopi.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/acces-au-formulaire.html
Fichier Edition Affichage Favoris Outils ?
Accès au formulaire " Réponse graduée, j'ai reçu ...
responsables
Nouvelles libertés, nouvelles responsabilités
Accès au formulaire " Réponse graduée, j'ai reçu un mail "
INFORMATION IMPORTANTE : Si vous recevez un mail de l'Hadopi, ou se faisant passer pour un mail de l'Hadopi, ne répondez jamais en faisant "répondre" à ce mail. Vous pouvez entrer en contact avec l'Hadopi via le formulaire accessible en bas de page ou par téléphone, ne répondez jamais directement aux mails de recommandation.
Il y a déjà des doutes...
Vérifier si le mail que vous avez reçu est bien une véritable recommandation de l'Hadopi.
Savoir comment faire valoir vos observations auprès de la Commission de protection des droits
Télécharger le formulaire pour faire valoir vos observations.
Vérifier si le mail que vous avez reçu est bien une véritable recommandation de l'Hadopi.
Avant d'entrer en contact avec l'Hadopi, les questions / réponses ci-dessous vous permettent de vérifier si le mail que vous avez reçu est bien un mail de recommandation de l'Hadopi. En répondant par oui ou par non vous pouvez faire cette vérification.
1/ La recommandation comprend elle bien votre adresse postale telle qu'elle apparaît sur les factures de votre FAI ?
Oui Non
Savoir comment faire valoir vos observations auprès de la Commission de protection des droits
Nouvelles libertés, nouvelles responsabilités signifient également nouvelles interrogations.
N°Cristal 09 69 32 90 90
Du lundi au vendredi, de 9h à 19h.
Si vous souhaitez contacter l'Hadopi pour d'autres raisons, merci de vous référer au formulaire de contact en cliquant ici.
P2P ? Wifi ? Phishing ?
Des interrogations sur un terme ? Consultez le glossaire.
Glossaire
Internet | Mode protégé : activé
100%

Hadopi

Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet

Recommandation de la Commission de la Protection des Droits de la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi)

Dossier n° xxxxx
Date : xxxx

Madame, Monsieur,

Attention, votre accès à Internet a été utilisé pour commettre des faits, constatés par procès-verbal, qui peuvent constituer une infraction pénale.

En effet, votre accès internet a été utilisé pour mettre à disposition, reproduire ou accéder à des œuvres culturelles protégées par un droit d'auteur. Cette situation rend possible leur consultation ou leur reproduction sans autorisation des personnes titulaires des droits. De telles consultations ou reproductions, appelées couramment « piratage », constituent un délit sanctionné par les tribunaux.

Cette utilisation a pu intervenir sans votre permission ou à votre insu, peut-être même par un usager non averti. Mais dans tous les cas, en tant que titulaire de l'abonnement à internet, vous êtes légalement responsable de l'utilisation qui en est faite*.

Vous devez en effet veiller à ce que cet accès ne fasse pas l'objet d'un usage frauduleux, en prenant toute précaution pour le sécuriser. C'est une obligation légale, sanctionnée par les tribunaux si elle n'est pas observée**.

Que vous reproche-t-on ?

On vous reproche un manquement à votre obligation de surveillance.

Ainsi, dans votre cas :

- Des agents assermentés ont constaté que le xxxxx une ou plusieurs œuvres protégées étaient reproduites, consultées ou offertes en partage depuis l'accès à Internet correspondant à l'adresse IP n °xxxxxxxx.
- Cette adresse avait été attribuée à ce moment par la société xxxxx, votre fournisseur d'accès à Internet, à :

[Coordonnées]

Que risquez-vous ?

Si, en dépit de cette recommandation vous invitant à prendre, dans les meilleurs délais, toute mesure utile et faute de mettre en œuvre, de façon effective, un ou plusieurs moyens de sécurisation de votre accès à Internet, de nouveaux manquements à votre obligation de surveillance venaient à être constatés, une contravention de négligence caractérisée pourrait être constituée à votre égard. Le juge judiciaire, saisi par l'Hadopi, pourrait alors prononcer une suspension de cet accès ainsi que, le cas échéant, une peine d'amende.

Quels sont vos droits ?

Vous pouvez obtenir des précisions sur les œuvres consultées, offertes en partage ou reproduites à partir de votre accès internet et, le cas échéant, formuler des observa s, en contactant l' pi :

- par voie électronique, en utilisant le f e accessible à l'ad
- par courrier postal, adressé à l'Ha on de 7
PARIS, en utilisant le même formulair
- par téléphone, au 09 69 32 90 90 (a

Dans ce cas, vous devez obligatoire un os ut d
message.

Pourquoi protéger le droit des aute

Sous les apparences séduisantes pra oit
auteurs des œuvres privent, en effet, ur j ution re, inte n g
danger pour l'économie du secteur sur créati listique, sous toutes
formes, qui est en cause. Pour mieux c les ages d'internet et le respect de la création, nous vous rappelons que des services en lig de plus en plus nombreux proposent aujourd'hui des offres légales attractives et respectueuses des droits des créateurs.

Informations

- Le rôle de l'Hadopi n'est pas de sanctionner : lorsqu'un dossier le justifie, l'Hadopi le transmet au juge qui seul peut prononcer une sanction.
- En aucun cas l'Hadopi ne réclame de somme d'argent. Toute demande en ce sens relèverait d'une tentative d'escroquerie de personnes malveillantes.
- Vous pouvez consulter le site de l'Hadopi www[.]hadopi[.]fr pour obtenir des informations sur ses missions, sur le dispositif applicable, sur l'offre légale et sur les moyens de sécurisation.
- Vous pouvez également demander des informations sur les moyens de sécurisation à votre fournisseur d'accès internet.

Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

La Commission de Protection des Droits de l'Hadopi

Annexes

Code de la propriété intellectuelle

*Article L. 336-3 du code de la propriété intellectuelle :
« La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.
« Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1.

** Article R. 335-5 du code de la propriété intellectuelle

I.-Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1° Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;

2° Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.-Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1° En application de l'article L. 331-25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

2° Dans l'année suivant la présentation de cette mmandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les perso s cou nt, en outre, être condamnées à la tain mmunication au public en ligne uxin e l'article L. 335-7-1.

re

nvi aux lib s (articles 39 et 40)

ract des Droits de l'Hadopi
lan
ion pr uvres sur Internet ». Vous bénéficiez d'un
n d ces données.
vous pouvez écrire à la présidente de la Commission de Protection des Droits en joignant une copie d'une pièce d'identité à l'adresse ci-dessus mentionnée en précisant sur l'enveloppe : « droit d'accès ».

Ce n'est pas un mythe...

Jeux d'argent… La mise en œuvre

Revue de détail

Réglementation reposant sur un agrément des plates-formes dites « légales »

Impact

Responsabilité pour accès non autorisé

Responsabilité pour accès autorisé (temps de pause)

- perte
- addiction….

Plan d'actions

1. Outils (filtrage)
2. Monitoring des outils
3. Information
4. Déclaration
5. Réaction notification

Secret défense… La mise en œuvre

Revue de détail

Arrêté du 23 juillet 2010 + Annexe = Instruction générale inter ministérielle sur la protection du secret de la défense nationale

Impact

Dispositions spécifiques SI

Impose des dispositions contractuelles

Plan d'actions

1. Mise en œuvre

2. Inspiration

Sécurité SI des AA … (RGS)

Revue de détail

Décret 2 février 2010

Arrêté 6 mai 2010

Impact

Conformité depuis 7 novembre 2010

Conformité au 7 mai 2011 pour SI 1 an

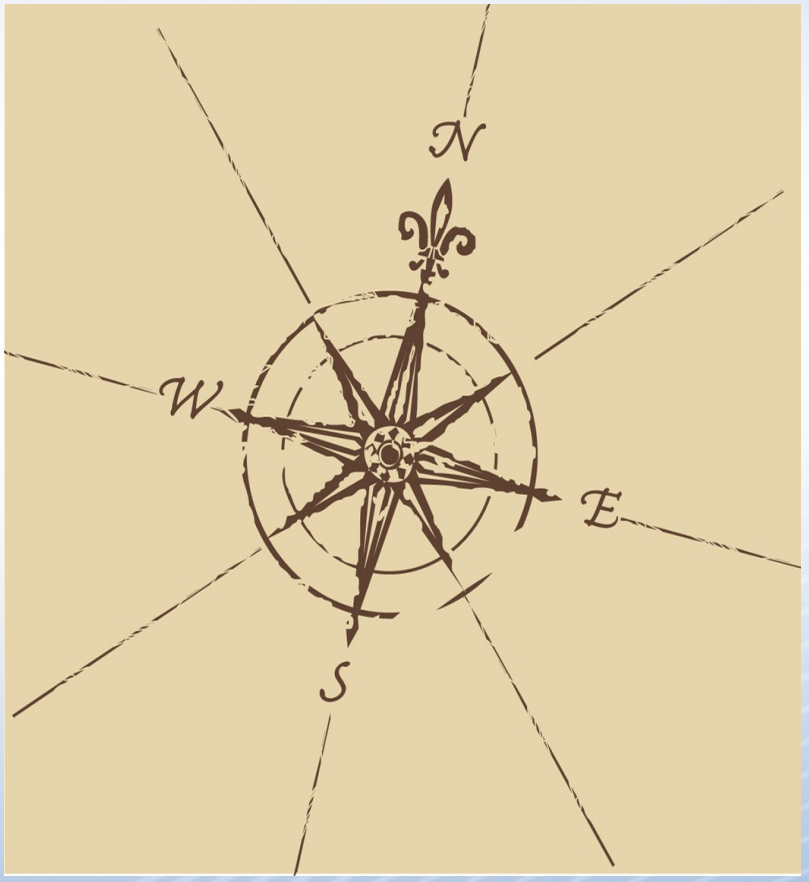
Conformité au 7 mai 2013 pour SI antérieur

Plan d'actions

1. **Opposabilité**
2. **Analyse de risque**
3. **CC pour SI a venir**
4. **Plan de conformité**
5. **Audit interne**

3. Evolution jurisprudentielle

1. Cybercriminalité
2. Cybersurveillance



Le droit de réguler

- Les chartes et les codes reconnus par les tribunaux
- Les sanctions sont possibles sur cette seule voie
  - Affaire : Coca Cola

Contentieux réseaux sociaux

- Jurisprudence Boulogne
  - De tes amis sur facebook tu te méfieras
- Jurisprudence Béthune
  - La clause de confidentialité s'étend à internet et limite la libre expression du salarié

Les jurisprudences moins classiques

- Jurisprudence Cnil
  - Vidéo-surveillance
  - Biométrie
- Autres AAI (en développement)
  - Hadopi, Arjel …
  - CSA, Arcep,

La Cnil 2010

Ca n'arrive pas qu'aux autres !

- Délibération 22 avril 2010 – Stop un système de vidéosurveillance
- Délibération 22 avril 2010 – Avertissement sur « commentaires »
  - L'horreur des blocs notes, un risque pour tous
- Délibération 18 mars 2010 – Stop un système biométrique

4. Evolution normative

1. Normes et références
2. Cohérence globale
3. Nouvelle donne juridique

Référentiel général de sécurité

- Triple impact
  - Pour les « AA » - Administration, Collectivité territoriale
  - Pour les prestataire qui travaillent avec les AA sur leurs SI
  - Acteurs techniques (certificats électronique et crypto)
- S'appliquent aux SI en mode « dialogue » - A/A & A/C
- Règles minimale + bonnes pratiques + prestataires agréés
- Référence à la norme 27001

Référentiel général de sécurité – Mise en œuvre

- Calendrier de mise en œuvre
  - 3 ans pour les SI antérieur au 6 mai 2010
  - 1 an pour les SI nés dans les 6 mois du RGS soit entre le 6 mai et le 6 novembre
  - Zéro an pour les autres

- Conséquence de la non mise en œuvre
  - Dans le texte : aucun
  - Manquement pour la « victime »

Normes 2700x

- Incidence juridique de la norme
  - Politique documentaire et mise à jour
  - Audit de risque
  - Politique « contractuelle » dédiée sécurité
  - Charte des personnels et charte administrateur

- La certification en marche
  - Actuel
    - Entreprises en cours de certification
    - Entreprises en renouvellement
    - Entreprises en « inspiration » (best practices)
  - Bientôt : Impact RGS étendu

Piqûre de rappel 2009 – Les 10 conseils Cnil pour sécuriser son SI

1. Adopter une politique de mot de passe rigoureuse
2. Concevoir une procédure de création et de suppression des comptes utilisateurs
3. Mettre en place le [illegible] automatique des postes
4. Identifier précisément qui peut avoir accès aux fichiers
5. Veiller à la confidentialité des données vis-à-vis des prestataires
6. Sécuriser le réseau local
7. Sécuriser l'accès physique aux locaux
8. Anticiper le risque de perte ou de [illegible]gation des données
9. [illegible]er et formaliser une politique de sécurité du système d'information
10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Pour mémoire...

La nouvelle donne 2010, Guide « La sécurité des données personnelles »

- Fiche 1 – Quels risques –
  - Action : Cartographie
- Fiche 2 – Authentifier les utilisateurs
  - Action : Politique identifiant (Login mot de passe ou plus)
- Fiche 3 – Habilitation et sensibilisation
  - Action : Profils et charte informatique + engagement
- Fiche 4 – Sécurité des postes de travail
  - Action : Firewall, antivirus et … limiter les « ports »
- Fiche 5 – Sécurisation de l'informatique mobile
  - Action : Chiffrement – Attention à la biométrie « La mise en œuvre de tels dispositifs est soumise à l'autorisation de la Cnil »
- Fiche 6 – Sauvegarde et PCA
  - Action : Mise en œuvre

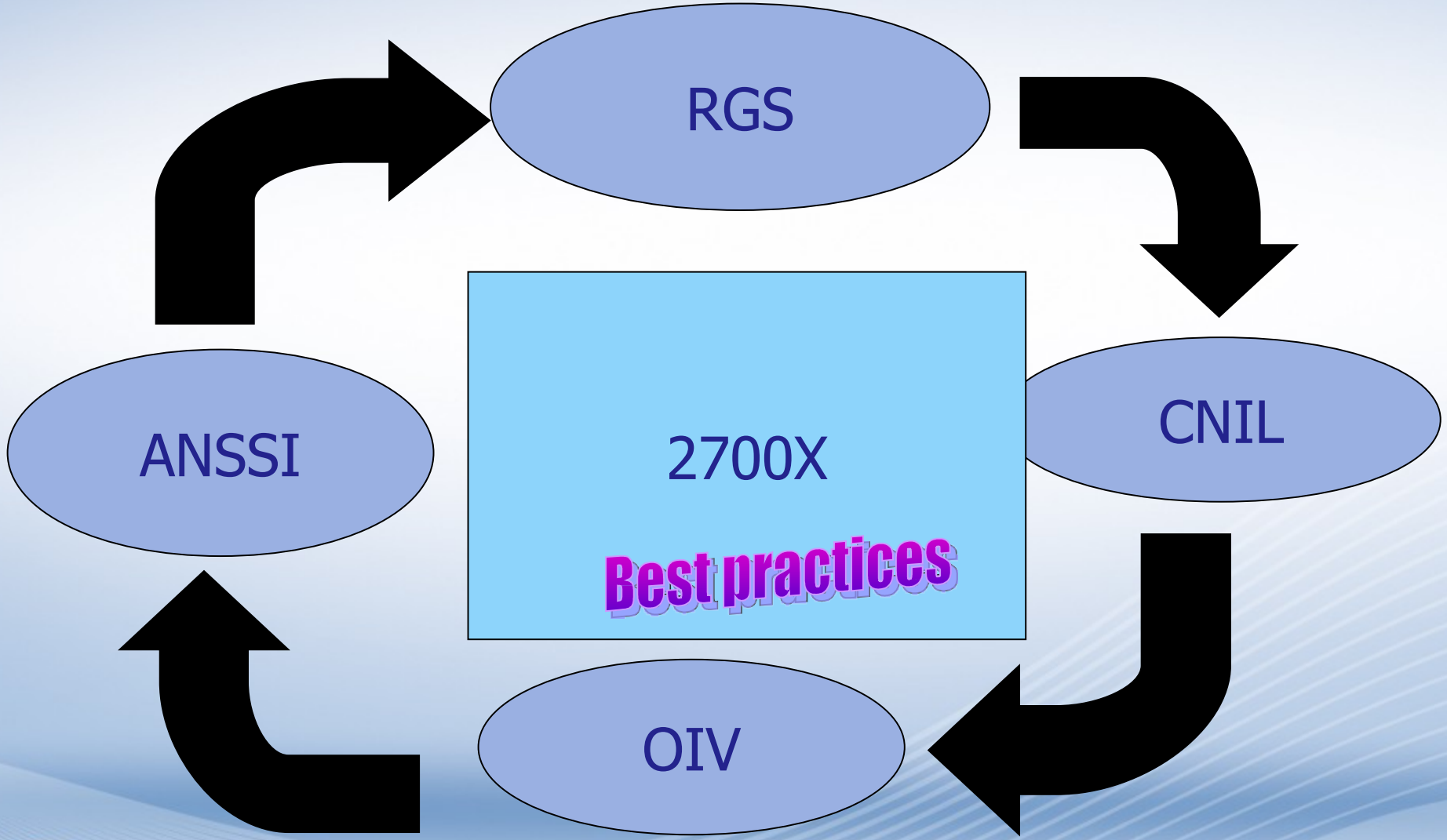
La nouvelle donne 2010, Guide « La sécurité des données personnelles »

- Fiche 7 – Maintenance
  - Action : Traçage et surveillance des opérations (main courante)
  - Action : Politique « rebut »
- Fiche 8 – Traçabilité et gestion des incidents
  - Action : Politique de « logs » 6 mois par principe
- Fiche 9 – Sécurité des locaux
  - Action : classique
- Fiche 10 – Sécurité du réseau interne
  - Action : « ce qu'il ne faut par faire… wi-fi »
- Fiche 11 – Sécurisation serveurs et applications
  - Action : Accès et administration renforcée
    - Charte administrateur

La nouvelle donne 2010, Guide « La sécurité des données personnelles »

- Fiche 12 – Sous-traitance
  - Action : clause + audit + restitution
    - Attention aux contrats de sous traitance
- Fiche 13 – Archivage
  - Action : Politique d'archivage et de destruction
- Fiche 14 – Echange d'informations
  - Action : ce qu'il ne faut pas faire « envoyer des données personnelles via Gmail et Hotmail »
- Fiche 15 - Développements informatiques
  - Action : Pensez données perso dès la conception
- Fiche 16 – Anonymisation
- Fiche 17 – Chiffrement

Cohérence-Cohésion

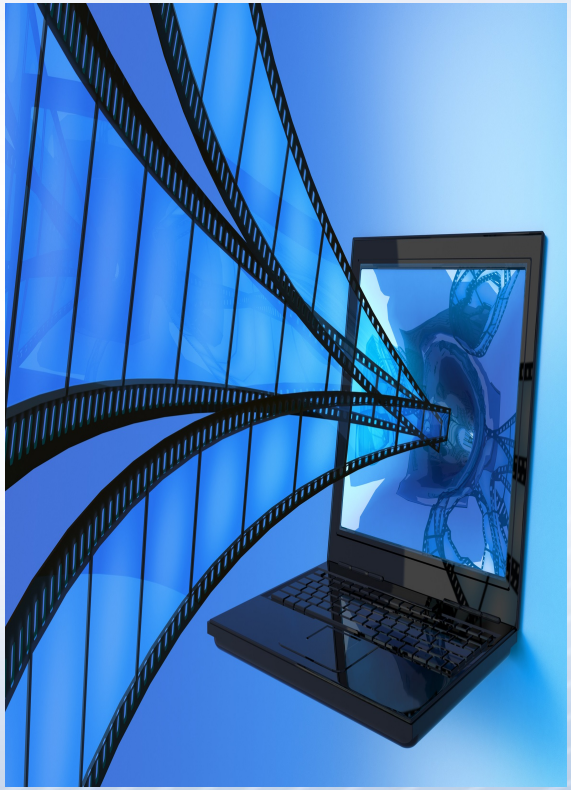


Et encore …

- RGI (Référentiel général d'interopérabilité)
- RGAA (Référentiel général d'accessibilité)
- Recommandations ANSSI
- Recommandations ENISA

5. 2011, accrochez vous …

1. En terme réglementaire
2. En terme de mise en œuvre
3. En terme de contrôle



Le nouvel article 34 ça pourrait être çà…

AVANT

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité
des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8. » - Art. 34 I&L

APRES

« Le responsable du traitement met en œuvre toutes les mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre toute violation entrainant accidentellement ou de manière illicite la destruction, le stockage, le traitement ou l'accès non autorisé ou illicite.

En cas de violation du traitement de données à caractère personnel, le responsable de traitement avertit sans délai le correspondant « Informatique et libertés » ou, en l'absence de celui-ci, la Commission nationale de l'informatique et des libertés. Le responsable du traitement, avec le concours du correspondant « Informatique et libertés », prend immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. Le correspondant « Informatique et libertés » en informe la Commission nationale de l'informatique et des libertés. Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, le responsable du traitement en informe également ces personnes, sauf si ce traitement a été autorisé en application de l'article 26. Le contenu, la forme et les modalités de cette information sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Un inventaire des atteintes aux traitements de données à caractère personnel est tenu à jour par le correspondant « Informatique et libertés »

Des décrets, (…)

Mise en oeuvre

Obligatoire ?

Donnée personnelle !

LOPSSI
Loi d'orientation et de programmation pour la performance de la sécurité intérieure

Revue de détail

- Des trous à combler
- Une nouvelle infraction pénale
  - Usurpation d'identité
- De la vidéo-surveillance à la vidéo-protection
- La perquisition numérique
- … and so and so
  - Intelligence économique

Impact

- Protection de l'identité numérique
- Culture de l'identité numérique
- Vérification des systèmes de vidéo
- Veille et IE

Risques juridiques : formes multiples de l'identité
Projet de loi LOPSSI

- La difficulté d'application sur un plan juridique
  - Une utilisation
  - De l'identité d'autre
  - Mettant autrui en situation de risque juridique…

- Une nouvelle incrimination à venir :

  - «*Art. 222-16-1.* – Le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui, est puni d'un an d'emprisonnement et de 15 000 € d'amende».

  - «Est puni de la même peine le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de porter atteinte à son honneur ou à sa considération.»

Une nouvelle orientation juridique

- Episode 1 - Régulation
  - Tout repose sur la jurisprudence
- Episode 2 - Auto-régulation
  - Tout repose sur le « bon vouloir »
- Episode 3 - Techno-régulation
  - Tout repose sur la « technologie »
- Episode 4 - Régulabelisation
  - Hadopi : Label
  - Informatique et libertés : Label
  - Jeux d'argent : Agrément
  - RGS et secret défense : Label ou agrément …

6. Nouvelles menaces

1. Risques techniques
2. Risques d'image
3. Risques juridiques

Risques techniques : Vol d'information

Vol de matériel – contenus inside

Savez vous d'où vient la clef USB qu'on vous a donnée

Key logger

Risques techniques : nouvelles tendances

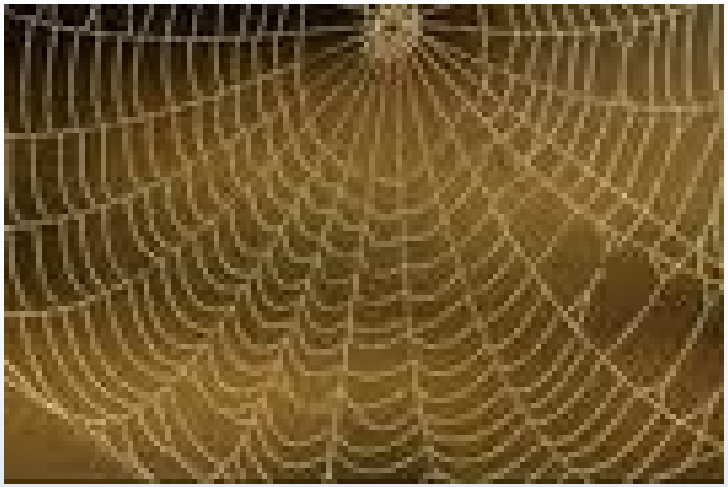
Connexions sauvages et responsabilité de l'abonné

Interception et mouchards

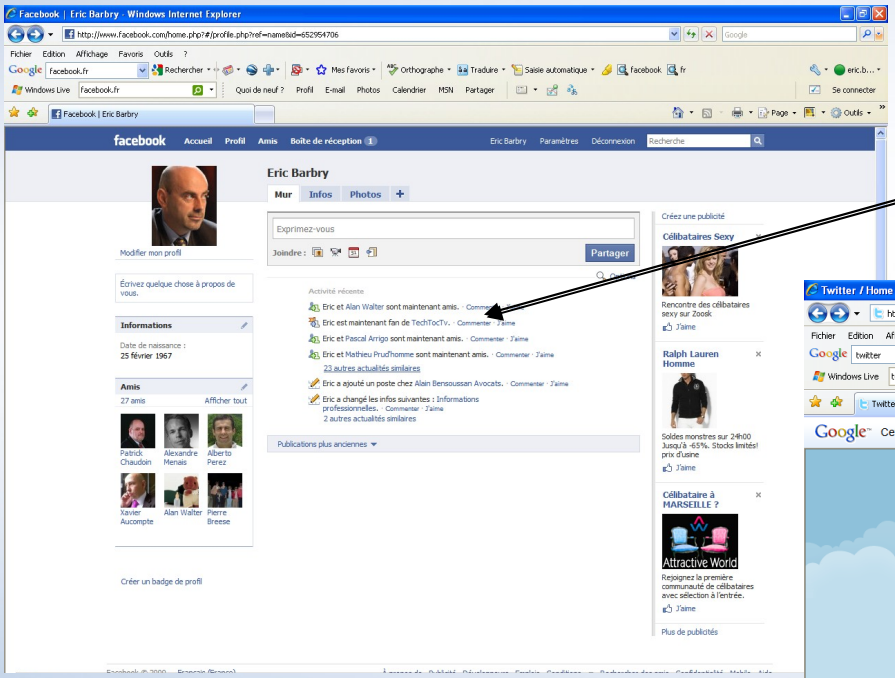
Nomade et anywhere …

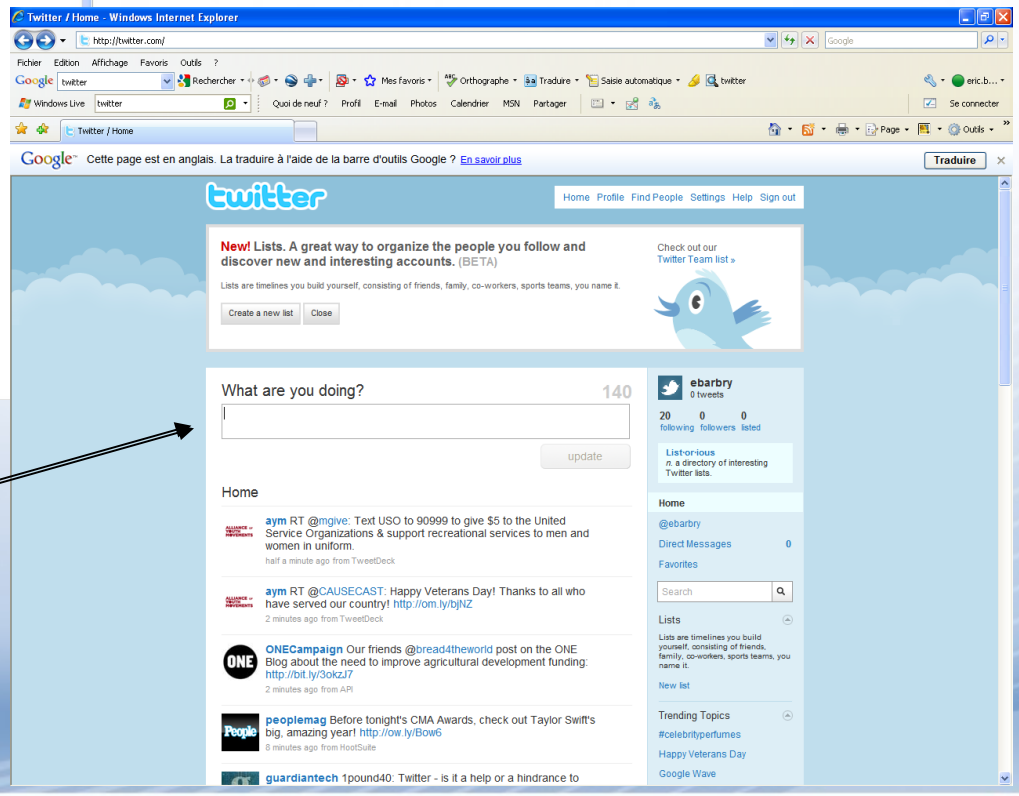
Risques d'image : +/- des réseaux sociaux

Pour le meilleur	Pour le pire
+ de visibilité	+ de Google hacking
+ d'échanges	+ de faux amis
+ de business	+ de fraude organisée
+ de benchmark	+ d'intelligence économique
…	…



Risques d'image ou pire...
What are you doing ?



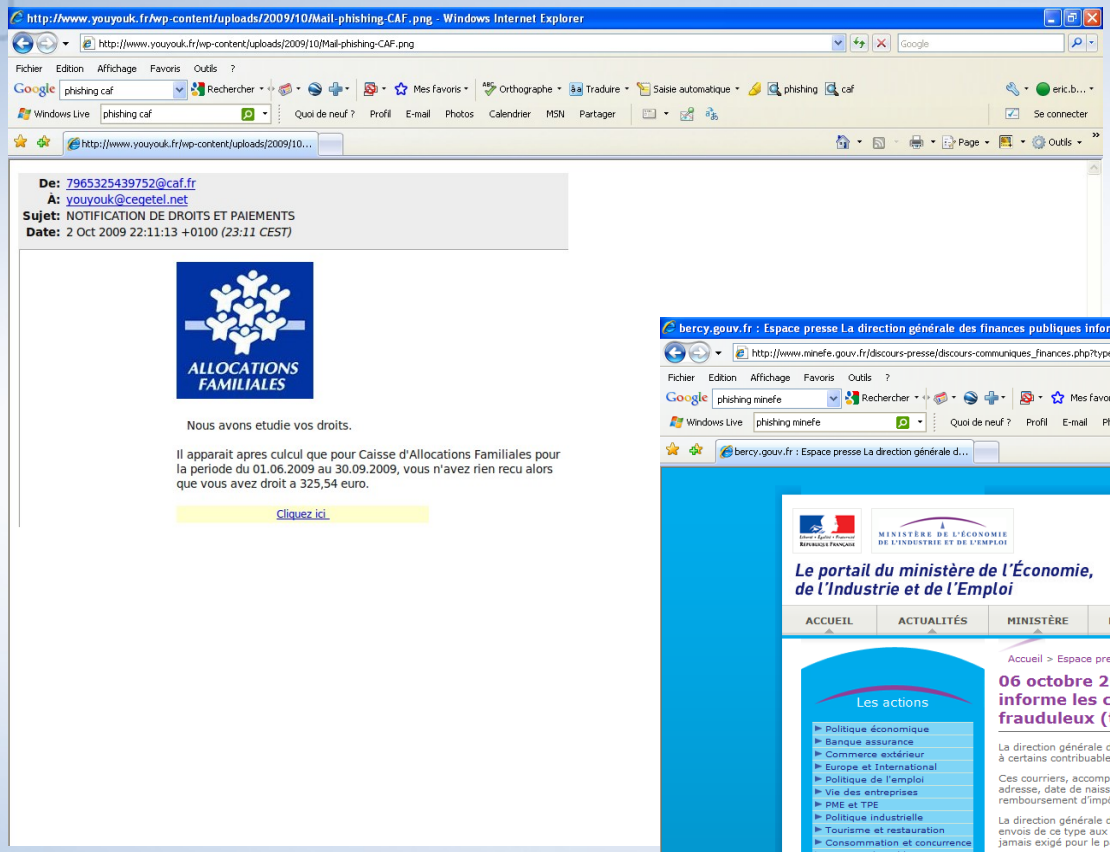


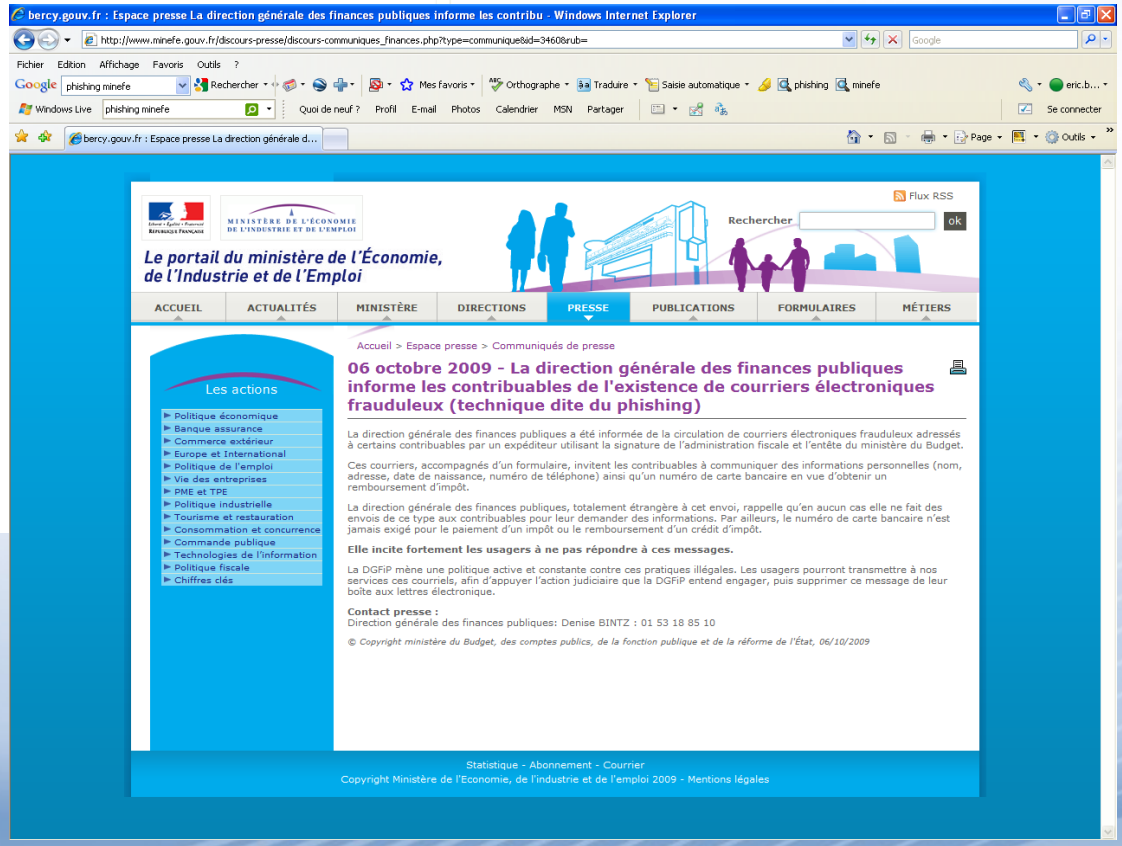
Risques juridiques : Usurpation d'identité

Risques juridiques : formes multiples de l'identité

Risques juridiques : le nouveau phishing

- Touche les salariés via les systèmes d'entreprise
  - Attaque ministère économie
- Se font passer pour l'entreprise elle-même
  - Ex: attaque via Université
- L'entreprise peut mettre en place des solutions
  - Même si elles sont faibles
- Mais elle doit réagir en bon professionnel
  - Information aux salariés sur les codes d'accès
  - Message d'alerte au cas par cas
    - Sans aller trop loin : émettre toutes réserves !


http://www.youyouk.fr/wp-content/uploads/2009/10/Mail-phishing-CAF.png - Windows Internet Explorer
De: 7965325439752@caf.fr
À: youyouk@cegetel.net
Sujet: NOTIFICATION DE DROITS ET PAIEMENTS
Date: 2 Oct 2009 22:11:13 +0100 (23:11 CEST)
ALLOCATIONS FAMILIALES
Nous avons etudie vos droits.
Il apparait apres culcul que pour Caisse d'Allocations Familiales pour la periode du 01.06.2009 au 30.09.2009, vous n'avez rien recu alors que vous avez droit a 325,54 euro.
Cliquez ici


bercy.gouv.fr : Espace presse La direction générale des finances publiques informe les contribu - Windows Internet Explorer
MINISTÈRE DE L'ÉCONOMIE DE L'INDUSTRIE ET DE L'EMPLOI
Le portail du ministère de l'Économie, de l'Industrie et de l'Emploi
Flux RSS
Rechercher
ok
ACCUEIL
ACTUALITÉS
MINISTÈRE
DIRECTIONS
PRESSE
PUBLICATIONS
FORMULAIRES
MÉTIERS
Accueil > Espace presse > Communiqués de presse
Les actions
Politique économique
Banque assurance
Commerce extérieur
Europe et International
Politique de l'emploi
Vie des entreprises
PME et TPE
Politique industrielle
Tourisme et restauration
Consommation et concurrence
Commande publique
Technologies de l'information
Politique fiscale
Chiffres clés
06 octobre 2009 - La direction générale des finances publiques informe les contribuables de l'existence de courriers électroniques frauduleux (technique dite du phishing)
La direction générale des finances publiques a été informée de la circulation de courriers électroniques frauduleux adressés à certains contribuables par un expéditeur utilisant la signature de l'administration fiscale et l'entête du ministère du Budget.
Ces courriers, accompagnés d'un formulaire, invitent les contribuables à communiquer des informations personnelles (nom, adresse, date de naissance, numéro de téléphone) ainsi qu'un numéro de carte bancaire en vue d'obtenir un remboursement d'impôt.
La direction générale des finances publiques, totalement étrangère à cet envoi, rappelle qu'en aucun cas elle ne fait des envois de ce type aux contribuables pour leur demander des informations. Par ailleurs, le numéro de carte bancaire n'est jamais exigé pour le paiement d'un impôt ou le remboursement d'un crédit d'impôt.
Elle incite fortement les usagers à ne pas répondre à ces messages.
La DGFiP mène une politique active et constante contre ces pratiques illégales. Les usagers pourront transmettre à nos services ces courriels, afin d'appuyer l'action judiciaire que la DGFiP entend engager, puis supprimer ce message de leur boite aux lettres électronique.
Contact presse :
Direction générale des finances publiques: Denise BINTZ : 01 53 18 85 10
© Copyright ministère du Budget, des comptes publics, de la fonction publique et de la réforme de l'État, 06/10/2009
Statistique - Abonnement - Courrier
Copyright Ministère de l'Economie, de l'industrie et de l'emploi 2009 - Mentions légales

Risques juridiques : gestion des droits

Note Ton Entreprise

Les entreprises vues de l'intérieur

Accueil | Noter ! | Entreprises | Recherche OK

Les entreprises vues par leurs employés

- Consultez les commentaires des employés
- Demandez des informations detaillées en privé
- Donnez votre propre avis

Note Ton Entreprise c'est :

- **5 880** entreprises notées
- **18 200** notations d'employés

J'Adore mon entreprise

Entreprise	Note	Evals
Svd Informatique	8.3	1
Sysinter	5.7	1
Nature Home	7.9	1
Spass Diffusion Ii	7.6	1
Escadre	6.3	2
Comareg	5.4	2

>> Suite des entreprises — Ajoutez votre entreprise ici !

Je Deteste mon entreprise

Entreprise	Note	Evals
Cat Amania	4.6	1
Dosisoft	4.3	1
Alexandra Plc	3.2	1
Carte Et Services	1.5	3
Cs	2.8	1
Performics	4.4	1

>> Suite des entreprises — Ajoutez votre entreprise ici !

Les dernières notes

Entreprise	Note
Neos-Sdi	3
Surcouf	1.3
Calleo Portage	5

Les plus notées

Entreprise	Note	Evals
Steria	3.7	150
Atos Origin	4	142
Capgemini	4.8	112

LesArnaques.com - Arnaques, Litiges, Conseils, Infos, Médiation, Coups de Gueule... - Windows Internet Explorer

http://www.lesarnaques.com/

Fichier Edition Affichage Favoris Outils ?

Google les arnaques Rechercher Partager Sidewiki Orthographe Traduire

Favoris Galerie de composants ...

LesArnaques.com - Arnaques, Litiges, Conseils, I...

Page Sécurité Outils

Les Arnaques .com

Soutenez-nous, faites un don!

Adresses utiles

Accueil Notre association Nous contacter

Forum

Fiches pratiques

- Achats et S.A.V.
- Communication
- Immobilier et Logement
- Banque, Crédit et Assurance
- Vos droits sur internet
- Justice
- Environnement
- Différentes normes
- Différents labels
- Modèles de lettres
- Divers

Google™ Recherche per

Les Nouvelles

Arnaques

23/09/2010 - Avertissemen

Nous souhaitons informer les internautes que la s

enquête de la

utres biens domestiques

ociété à responsabilité limitée

Gérant :

suite]

Internet

16/09/2009 - Communiqué de pres

Utilisation des liens sponsorisés par les con tion en vue «Etre sur Internet» ne suffit pas pour se

et utiliser au mieux les f

comme par

Conso

22/10/2009 - A

Bonjour, nous sollicitons votre vigilence lorsque vous effectuez un achat sur

ir que vous av

malheureusem tato...

[Lire la suite]

Les Arnaques .com Le Forum

Toutes les réponses à vos questions par les internautes et les membres de notre équipe sur le forum de LesArnaques.com

L'Editorial

Article 11 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 :

" La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déter-

Terminé

Internet | Mode protégé : activé

100%

FR 16:05 02/10/20

SurveillerMonSalarie.com – Surveillez l'ordinateur de votre salarié ! - Windows Internet Explorer

http://surveillermonsalarie.com/

Fichier Edition Affichage Favoris Outils ?

Rechercher Partager Sidewiki Connexion

Favoris Galerie de composants ...

SurveillerMonSalarie.com – Surveillez l'ordinateur...

Page Sécurité Outils

ACCUEIL | OFFRE | CONCEPT | INFOS PRATIQUES | CONTACT | LE BLOG DU PATRON

Besoin d'aide ? 02.38.98. 05.45

surveillermonsalarie.com

Concept

Les patrons pensaient qu'Internet et l'ordinateur en général étaient un outil de travail. Ils se sont lourdement trompés. C'est la conclusion assez

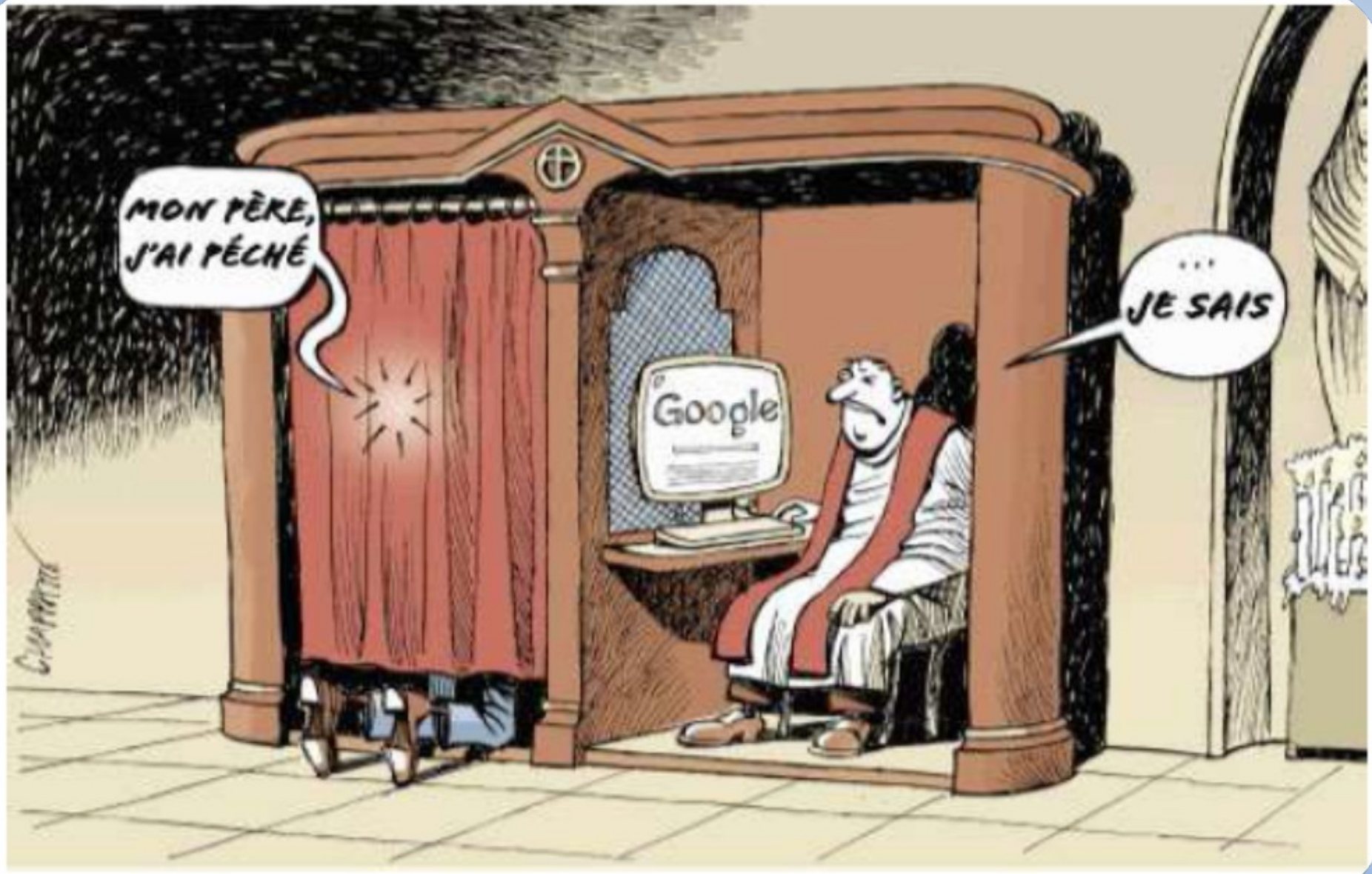
Offre

Surveillermonsalarie.com vous propose une solution simple d'emploi ! Vous aurez maintenant la possibilité de savoir ce que fait votre employé

Internet | Mode protégé : activé

100%

FR 19:36 03/10/2010


MON PÈRE, J'AI PÉCHÉ
Google
...
JE SAIS

Banksters & Marée noire

« retour à la liste

380 vues. | 6 com. | 7 fav.

Favori Partager Playlist Groupe Signaler

Votez !

J'aime 32 personnes aiment ça. Soyez le premier parmi vos amis.

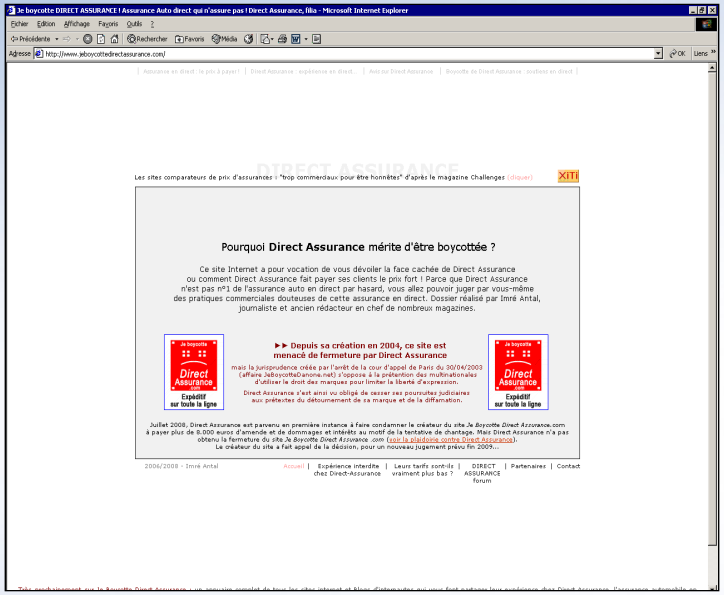
Ils massacrent le monde la planète sans êtres effrayés , ces salauds méritent la prison a vie! IL Y A TROP D' ENFANTS QUI SURVIVENT A LEURS NAISSANCES ET C'EST CATASTROPHIQUE POUR LA BIOSPHÈRE SELON DAVID ROCKEFELLER, LE PÉTROLIER-PHARMACO-BANKSTER.. PENDANT QUE LUI ET SES DÉGÉNÉRÉS D'AMIS MULTI-MILLIARDAIRES DÉVERSENT DU PÉTROLE DIRECTEMENT DANS LE GOLFE DU MEXIQUE..JE DÉTESTE CE MEURTRIER. IL A LES MAINS PLEINES DE SANG PAS SURPRENANT QU IL

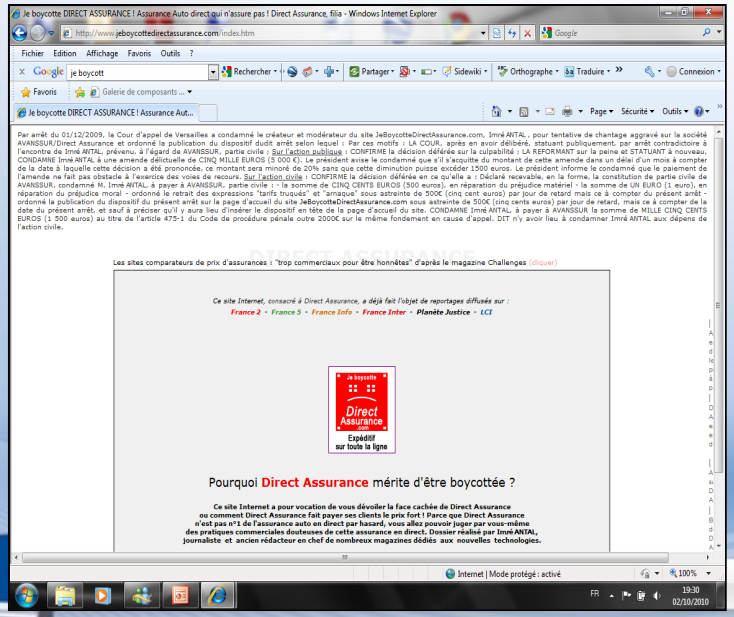
suite

Chaîne : Actu et Politique Publiée le : 02/05/10

Tags : Marée noir complot pétrole énergie primitive sale salauds pollueurs pollution banksters Rothschild

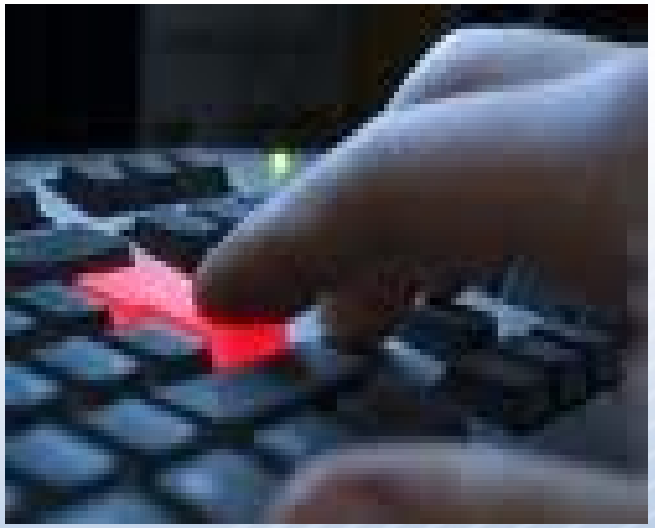
On vous nargue…





On ne vous oublie jamais…

IE généralisée



Clic fuite

ADMINISTRATEUR SYSTÈMES RESEAUX
BONNES PRATIQUES

Dessine moi un ASR…

1. Un ASR en droit
2. Un ASR en image

L’ASR … N’EXISTE PAS !

Le référentiel légal de l'Administrateur

- Référentiel légal « direct »
  - Arrêté 2010 sur la défense nationale
- Référentiel légal « indirect »
  - Cnil
    - Rapport employeur/employé
      - Fiche pratique 7
    - Rapport sécurité des données
      - Fiche pratique 4 et 11

Un premier pas – Référentiel Administrateur… sécurité

Les autorités qualifiées peuvent se faire assister par un ou plusieurs agents, responsables ou officiers de sécurité des systèmes d'information (ASSI, RSSI, OSSI) (148). Elles précisent, lors de leur désignation, le périmètre de leurs attributions et leur dépendance hiérarchique. Ce périmètre peut être un service, une direction ou un organisme, dans sa totalité, ou un ou plusieurs systèmes d'information, ou un établissement.

Ces agents assurent principalement les fonctions opérationnelles de la sécurité des systèmes d'information. Ils peuvent être notamment chargés :

— d'être les contacts privilégiés des utilisateurs du système pour les questions de sécurité ;

— d'assurer la formation et la sensibilisation des responsables, des informaticiens et des usagers en matière de sécurité des systèmes d'information ;

— de tenir à jour la liste des personnels ayant accès aux systèmes d'information

— de faire surveiller en permanence les activités des personnes extérieures appelées à effectuer des interventions sur les systèmes d'information ;

— de s'assurer de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites ;

— d'assurer leur sensibilisation aux mesures de sécurité et de les informer de toute modification des conditions d'emploi du système ;

— de veiller à la mise en œuvre des mesures de protection prescrites, d'établir des consignes particulières et de contrôler leur application ;

— d'assurer la gestion, la comptabilité et le suivi des ACSSI dans leur périmètre de responsabilité et d'en assurer périodiquement l'inventaire ;

— d'établir les consignes de sécurité relatives à la conservation, au stockage et à la destruction des ACSSI ;

— de vérifier périodiquement l'installation et le bon fonctionnement des dispositifs de sécurité ;

— de veiller au respect des procédures opérationnelles de sécurité propres au système d'information ;

— de surveiller les opérations de maintenance ;

— de rendre compte de toute anomalie constatée ou de tout incident de sécurité.

(Instruction générale interministérielle sur la protection du secret défense nationale)

Référentiel interne

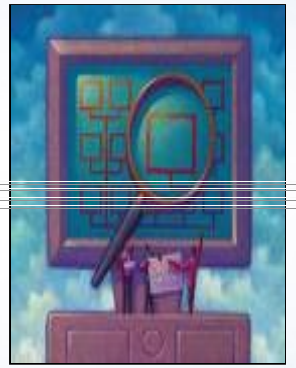
- Contrat de travail et fiche de poste
- Charte des systèmes d'informations
- PSSI – SDSSI – Politique log…
- Charte administrateur

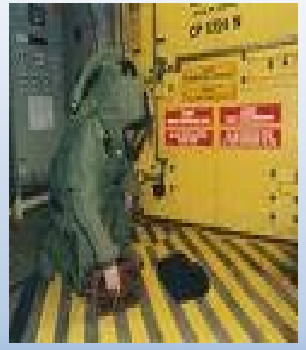
Référentiel jurisprudentiel « spécial » ASR

* « Si la préoccupation de la sécurité du réseau justifi[e] que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils dispos[ent] pour mener les investigations et prendre les mesures que cette sécurité impos[e], (…) par contre, la divulgation du contenu des messages ne relèv[e] pas de ses objectifs ». (CA Paris 17e ch. 17-12 2001 Ministère Public et A. T.)

* Un administrateur système réseau d'une association a été licencié pour faute grave après que son employeur ait découvert, par hasard, au cours d'un audit du réseau du système informatique de l'association, la présence de fichiers en provenance d'Internet sur le poste de l'administrateur indiquant un téléchargement 24h24 et 7 jours/7 ce qui portait à environ 6 Go d'images, de sons, de vidéos et de progiciels stockés sur son disque dur. La cour a considéré le licenciement pour faute grave justifié eu égard aux fonctions du salarié considérant que ce dernier avait « profité de ses fonctions et de l'accès privilégié au système informatique de son employeur pour, à l'insu de celui-ci, utiliser ce système à des fins personnelles étrangères à l'activité de l'association ». (CA Paris 4-10-2007 Mr Sixdeniers c/Association ARFP)

L’ASR en image …





Les fonctions de l'ASR

1. Les droits
2. Les obligations

Qui est le responsable ?

Vous peut être …

Responsabilité professionnelle

- Contrat de travail ou fiche de poste
- Politique de sécurité
- Charte des SI
- Norme et état de l’art

Responsabilité personnelle

- Agissement personnel
- Agissement en dépassement d'une délégation
- Refus d'appliquer un ordre légitime
- Application d'un ordre illégitime

Responsabilité partagée

- Co-responsabilité
- Complicité
- Cascade de responsabilité
- Employeur/employé

Droit d’agir et d’analyse

- Monitoring temps réel
- Analyse des logs
- Mise de main – avec l’accord de l’utilisateur
- Opération de contrôle

Peut ainsi :

- identifier des comportements illicites
- accéder à des contenus protégés

Droit d’intervenir

- Créé profil et habilitation
- Mise en place de solutions techniques (patch et autre)
- Maintien du service (ex : Code d’accès)
- Mesure d’urgence et de crise

- Participation à la « politique de sécurité »
- A le droit (devoir) de dire non ou au moins d’être couvert

Informer et former

- L'ASR ambassadeur des « bons usages »
- Informe
  - Utilisateurs
  - Hiérarchie
    - Évite de se transformer en « juriste »
- Reporting
  - Programmé
  - Sur situation identifiée

Alerte et mise en garde

- Le SI est un « produit dangereux »
- Alerte et mise en garde
- L'important n'est pas nécessairement d'être au « normes » mais d'informer sur les écarts
- Preuve de la remontée d'information

Obligation N°1 - Confidentialité

- Secret professionnel
- Secret défense
- Secret de fabrique
- Confidentialité

Obligation N°2 - Respect du droit des tiers

- Vie privée des tiers
- Propriété des tiers
  - Attention à la contrefaçon
- SI des tiers
  - On ne teste pas la sécurité des SI des tiers à l'insu de leur plein gré … même pour leur bien être ..

Obligation N° 3 - Collaboration et coopération

- Interne
  - Autorité habilitée
  - Enquêtes internes
- Externe
  - Police & justice
  - Autorités administratives indépendantes
  - ?? des autres (huissiers, experts, avocats,…)

Interdiction générale

Ecoute

Intrusion

Espionnage

Enquête

Vengeance

Les bonnes pratiques

1. Revue de détail

Bonne pratique 1 – Ne pas ignorer le droit

- L'ASR « baigne » dans le droit
  - Des SI – informatique + télécom + Internet (convergence)
  - Des données (secret, propriété, privé, …)
- Le droit est
  - De + en plus complexe
  - De + en plus exigent (sanction s'accroissent)
    - Ex : Informatique et libertés ou notice légale
- L'administrateur doit avoir des « réflexes juridiques conditionnés »
- L'administrateur n'est pas un juriste… et ce n'est pas grave ;-)
  - L'ASR ne doit pas se transformer en juriste interne ce n'est pas son job
  - L'ASR ne peut pas être son propre avocat
    - Profession réglementée
    - "The man who is his own lawyer has a fool for his client"

« EN SAVOIR ASSEZ POUR NE PAS EN FAIRE TROP »

Un droit particulier de la sécurité…

BUDAPEST 2001	**Lutte contre le terrorisme 2006**	**Hadopi Téléchargement 2009**	**Loi sur les jeux d'argent 2010**	UE
	SOX Sociétés cotées 2002	**Bale II (secteur bancaire) 2004**	**Solvency II (secteur assurance) 2008**	Infrastructures Européennes essentielles
	LSF Sécurité financière 2003	**LCEN Internet 2004**	**Informatique & Libertés II 2004**	Décision cadre 2005/222/JAI Attaques SII
	STAD Fraude informatique 1988	Loi **sécurité** Quotidienne (LSQ) 2001	Loi **sécurité** Intérieure (LSI) 2003	Règlement 460/2004 Création ENISA
				Décision cadre 92/242/CEE – Sécurité des SI

Normes et standards – ISO 27001 et s.

Bonne pratique 2 – Pratiquer la veille juridique

- La veille est une des fonctions des ASR
- La veille technique est la base
- La veille juridique s'impose
  - La vérité d'hier n'est pas forcément celle de demain
    - Ex 1 – Accès aux mels
    - Ex 2 – Images pornographiques en entreprise
- Les sources de veille sont nombreuses
  - Ex : www.legalis.net - www.juriscom.net – www.cnil.fr – www.ssi.gouv.fr
  - Ex : www.alain-bensoussan.com

« UN ASR AVERTIT EN VAUT DEUX »

Bonne pratique 3 – Disposer d'une boite à outils juridiques

- Une bonne administration passe par la mise en œuvre d'outils techniques, organisationnels mais aussi juridiques
- Ces outils sont « demandés » (ex : Cnil) et « reconnus » (ex : Charte)
- Les outils dépendent des travaux que l'on veut mener
- Il n'y a pas que l'outil qui compte mais aussi la manière de s'en servir

« UN BON OUVRIER A TOUJOURS SES OUTILS »

Bonne pratique 4 – Ne pas faire … ce que tu n'as pas le droit de faire

- La liste n'est pas si longue
- La plupart du temps c'est du bon sens
- Agir sur ordre
- Documenter son action

« NE FAIT PAS A AUTRUI CE QUE TU NE VOUDRAIS PAS QU'ON TE FIT »

Bonne pratique 5 – Ne pas être négligent fautif

- Les trois piliers de la responsabilité
- Risque majeur pour ASR = 1383 c'est la négligence fautive
- Négligence fautive en 2 mots : Manque de vigilance et de clairvoyance
- Tryptique = info / contrôle / action

« NE PAS OUBLIER LE TRYPTIQUE DES ASR HEUREUX

Bonne pratique 6 - Prouver que l'on fait bien son travail

- Savoir + Savoir faire ne suffisent pas
- Importance du « Faire savoir »
- Besoin interne
- Besoin externe

« ASR POUR VIVRE HEUREUX VIVONS NON CACHES »

Bonne pratique 7 – Connaître et utiliser la « bonne chaîne »

- Information – Dénonciation – délation
- L'obligation de dénoncer pour tous
- L'obligation spéciale « fonctionnaires »
- L'ASR n'est pas un électron libre, l'information passe par la chaîne d'alerte

ASR UN MAILLON CERTES MAIS UN MAILLON ESSENTIEL

Bonne pratique 8 - Savoir coopérer avec les autorités compétentes

- En dehors de l'interne coopération avec les autorités type police, gendarmerie, contrôle Cnil, contrôle préfecture (vidéosurveillance) ;
- Pas le droit de ne pas collaborer ;
- Pas nécessaire pour autant de jouer en solo;
  - Savoir répondre et informer la chaîne fonctionnelle ;
    - (cf alerter la chaîne Bonne pratique 7)
- Surtout pas en donner plus que ce qu'on doit donner (ex : réquisition judiciaire) + attention au secret professionnel et à des secrets spécifiques (secret défense)

« Informer ou cautionner … il faut choisir »

Les outils au service de l'Administrateur

1. Outils organisationnels
2. Outils techniques
3. Outils juridiques

« L’action visant à prévenir les non-conformités est souvent plus rentable que l’action corrective »

Norme 27001 (p 13)

Outils organisationnels

- Audit de risque
- Politique ou SD sécurité
- Politique de logs
- PCA/PRA…
- Chaîne d'alerte

Conformité légale

Information
- Personnel
- IRP

Déclaration
- AAI
- Tutelle

Outils techniques

- Badges
- Login/password
- Biométrie
- Géolocalisation
- Vidéo
- Crypto
- Certificats électroniques
- OTP
- Enregistrement son
- RFID
- Filtres
- ++ logs

Etude de proportionnalité

Etude d'impact

Conformité légale

Information
- Personnel
- IRP

Déclaration
- AAI
- autres

Outils juridiques au service de l'ASR

Tableau de bord de l'ASR

La boîte à outils de l'ASR

Code de l'ASR

Norme 27 (A15)

RGS

CNIL

Assurance

Engagements

Code de l'ASR

Mise à jour programmée

RL General

RL Métier

Mise à jour immédiate

La boîte à outils de l'ASR

EVALUATION

Charte informatique et libertés	**Charte éthique**	**Code de la sécurité**
Guide opérations de contrôles	**Conditions générales de sécurité**	**Plan de sensibilisation**
Charte accès tiers	**Charte administrateur**	**Autres Chartes** **Ex : poste Libre service Télé-travail**
Charte des personnels	Livret technique	Guide utilisateur

MCO

Les 4 risques majeurs …

- Risque 1 - Disposer d'une « vieille » charte
  - Inadaptée techniquement
  - Inadaptée opérationnellement
    - Protection illusoire - Mode boomerang
- Risque 2 - Ne pas disposer d'une charte administrateur
  - Responsabilité employeur agissement admins
  - Refus des admins sur les contrôles
- Risque 3 – Absence de Guide opérations de contrôle
  - Prendre un risque sur l'opération
  - Rendre la preuve nulle
- Risque 4 – Absence de Conditions générales de sécurité
  - L'entreprise est pourtant aussi responsable des « prestataires »
    - Art 35 de la loi informatique et libertés
    - Rappel de l'ANSSI sur la sous-traitance

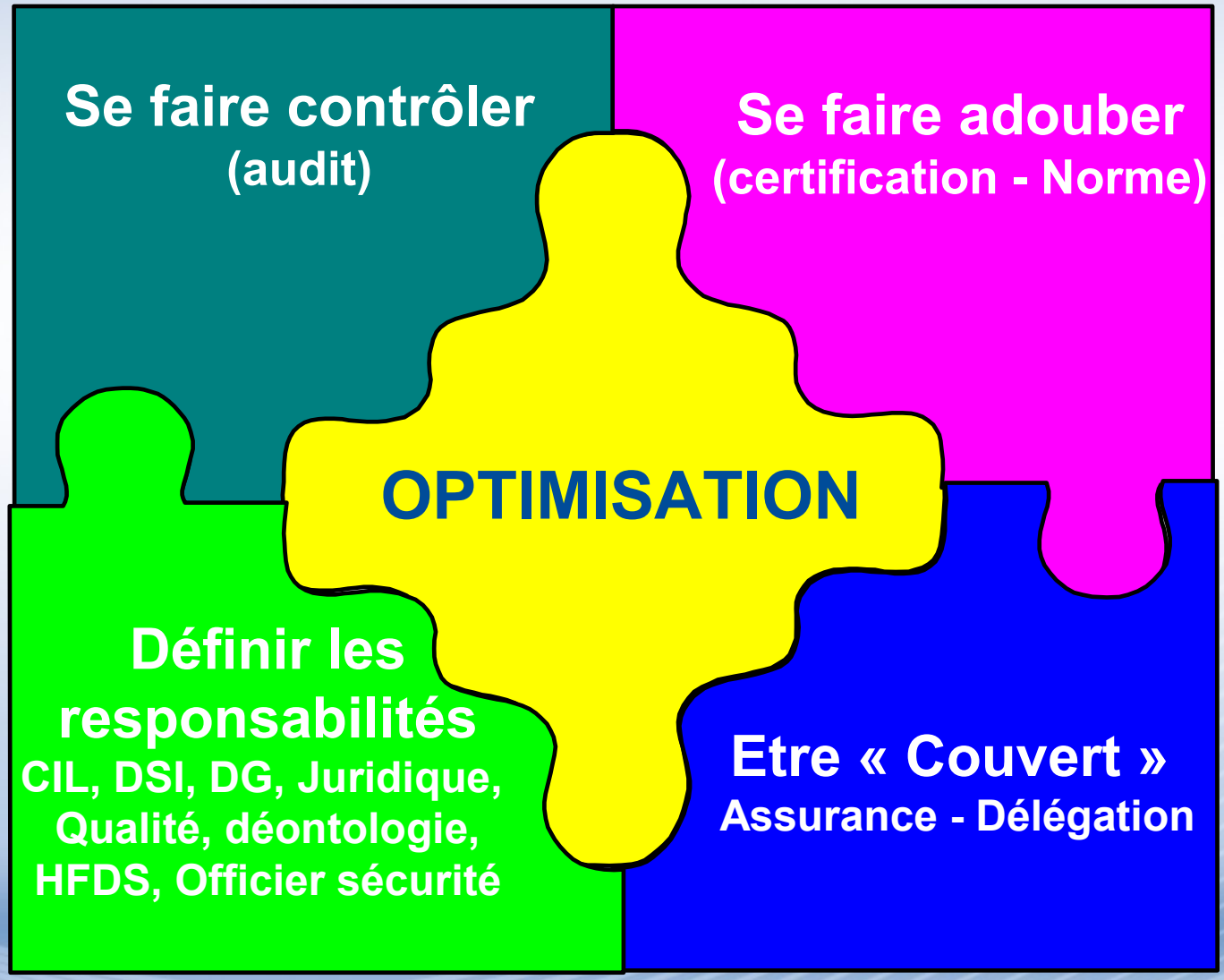
Tableau de bord de l'ASR

Une nouveauté ? → Une action ?

On ne rattrape pas le temps perdu…

… ou alors avec un budget conséquent

Maîtriser des risques



Le secret du bonheur pour un ASR

S'intéresser au droit …

Avant que le droit ne s'intéresse à lui

Cinq conseils

- Disposer d'un code de l'ASR
- Disposer d'un tableau de bord juridique
- Disposer d'une charte utilisateur 4G
- Disposer d'un guide des opérations de contrôle
- Disposer de « CGS » (conditions générales sécurité)

Contact

- ALAIN BENSOUSSAN AVOCATS
  29 rue du colonel Pierre Avia Paris 15è
  
  Tél. : 33 1 41 33 35 35
  Fax : 33 1 41 33 35 36
  
  paris@alain-bensoussan.com

- Eric Barbry
  
  L.D. : 33 1 41 33 35 27
  Mob. : 33 6 13 28 91 28
  
  eric-barbry@alain-bensoussan.com

Crédit photo

- Conception et réalisation du support
  - Alain Bensoussan avocats © 2010

- Crédits photos
  - ©ioannis kounadeas-fotolia.com
  - ©cybrain-fotolia.com
  - ©nabil biyahmadine-fotolia.com
  - ©david_hoepfner-fotolia.com
  - ©alphaspirit-fotolia.com
  - ©foto-fritz-fotolia.com
  - ©michael brown-fotolia.com
  - ©fribourg -fotolia.com

MERCI