Fourniture d'accès à Internet et au réseau local : droits et obligations des établissements publics d'enseignement supérieur

Estelle De Marco

Inthemis

JRES 2011
Toulouse, mercredi 23 novembre 2011

Introduction

- **Qualités de l'établissement fournissant un accès**
  - **Etablissement public chargé d'un service public**
  - **Employeur**
  - **Abonné** à Internet
  - **Fournisseur d'accès à Internet ? (FAI)**
    - ✓ Oui pour la conserv. de données d'identification (CA Paris 05)
    - ✓ Conserv. données de trafic -CPCE : FAI "à titre accessoire"
    - ✓ NSP s'agissant des autres dispos LCEN / CPCE
- **Droits/obligations en termes de :**
  - Sécurisation du SI et de son utilisation
  - Contribution à la lutte c/ les infractions / contenus illégaux

Droits et obligations de sécurisation du système d'information et de son utilisation

Les obligations de sécurisation

Obligations… liées à la qualité de la personne - ex.

- **Autorités administratives : respecter le RGS**
  - **Textes :** ord. 12/2005 ; décret 02/2010 ; arrêté de 05/2010 (approuvant RGS version 1.0)
  - **Contenu :** règles auxquelles les SI des AA (dont EPES) doivent se conformer
  - **Domaine concerné :** sécurité des échanges…
    - entre autorités administratives et usagers,
    - entre autorités administratives,
    - sauf SI relevant du secret de la défense nationale
  - **Mise en conformité obligatoire :** 12 mois (SI créés dans les 6 mois de la publication) / 3 ans (SI antérieurs)

Obligations de sécurisation … liées à la qualité de la personne (suite)

- Référentiel général de sécurité (suite)
  - **Contenu de l'obligation** (décret) **:** dans conditions RGS,
    - **1° Identifier l'ensemble des risques** (SI et infos)
    - **2° Fixer les objectifs de sécurité**
    - **3° En déduire les fonctions de sécurité - leur niveau**
    - **4° Respecter les règles correspondantes** du RGS
    - **5° Réexaminer régulièrement la sécurité SI + infos**
  - **Avant mise en service opérationnelle du SI : homologation de sécurité**
    - ✓ Attestation d'aptitude du SI à entrer en service
    - ✓ En informer les utilisateurs

Obligations… liées à la qualité de la personne (suite)

- **Opérateur :** (rappelé en 2011)
  - **Secret des correspondances, neutralité et intégrité des messages** (+ info du personnel)
    → **EPES ?** – sanctions pénales (pers. chargées d'un SP)
    – Info du personnel conseillée (chartes)
  - **Intégrité / sécurité réseaux ouverts au public**
    → Un contrôle de la sécurité / de l'intégrité des réseaux / services peut être imposé par le ministre
    → **EPES ?** - a priori non, mais intérêt à la sécurité des réseaux (dont risques en termes de resp^{té}…cf. infra)

Obligations… liées à la nature des données - exemples

- **Nombreuses autres obligations selon la nature des données :**
  - ➢ conservation/archivage,
  - ➢ obligations contractuelles,
  - ➢ sécurité des données à caractère personnel…

→ Et nouvelle obligation pour les opérateurs de notifier à la CNIL toute violation de DCP (cadre not. conservation des données de trafic) – O^{ce} août 2011

→ EPES : ? – mais 5 ans / 300 000 euros

Obligations… liées à la nature des données (suite) - exemples

- **Obligation de sécurisation c/ la contrefaçon**
  - **Contravention de négligence caractérisée :**
    - L'HADOPI (CPD) constate une contrefaçon → 1ère reco. de mettre en œuvre un moyen de sécurisation,
    - Nouvelle contrefaçon dans l'année via cet accès

      ET, « sans motif légitime » :
      - ✓Soit l'EPES n'avait pas mis en place ce moyen,
      - ✓Soit il a « manqué de diligences » dans la mise en œuvre de ce moyen

    → Motifs légitimes ? Moyen de sécurisation labellisé / autre moyen ? Manqué de diligences ? → juge

Obligations… liées à la nature des données (suite) – exemples

- Obligation de sécurisation c/ la contrefaçon
  - **Sanctions de la négligence caractérisée**
    - ✓ Contravention 5ème classe (1500 euros) +
    - ✓ suspension de l'accès pendant 1 mois +
    - ✓ interdiction de souscrire un autre contrat sur cette période (3750 € amende) +
    - ✓ charge du prix de l'abonnement ou de la résiliation

    → **Le juge peut ne pas appliquer la suspension**
  - **Suspension d'accès : aussi 1 peine complémentaire de la contrefaçon**
    - ✓ Durée maximale d'un an,
    - ✓ mêmes interdictions (autre contrat /coût abonnement)

Le droit de sécuriser le système d'information et son utilisation

Sécurisation du SI et de son utilisation – le droit de sécuriser

- **Enjeu : renforcer la sécurité juridique de l'EPES** (hors confiance des tiers, patrimoine…)

Responsabilité = essentiellement :

- ✓ Violation d'1 obligation de sécurisation (EP, psdt, agent)
- ✓ Infraction, non respect d'une autre obligation légale
- ✓ Faute personnelle (agent)
- ✓ Faute agent cadre service / fait d'1 tiers + dommage (EPES)
- ✓ Sans faute (carence dans organisation SP - EPES)

DONC : pot. toute faille / mauvaise utilisation des accès

FONDEMENT (hors respect loi) : Etat de l'art (normes, RGS, recommandations DCSSI / CNIL…)

Sécurisation du SI et de son utilisation – le droit de sécuriser (suite)

- **Responsabilité pénale : exemples …**

➢ **Chef d'établissement :** défaut de formation des employés permettant d'assurer la sécurité de données personnelles (cass. crim 01)

➢ **Agent :** utilisation d'un logiciel contrefait ; mise à disposition sans droits

➢ **RI ? :** complicité en cas d'infraction continue, si connaissance + inaction (ex. recel de contrefaçon) → mais complicité par inaction rarement admise

➢ **Tiers** auteur d'une intrusion informatique – **sauf en l'absence de sécurisation** *(CA Paris 02)*

Sécurisation du SI et de son utilisation – le droit de sécuriser (suite)

- **Responsabilité pour faute (civ. ou admin.) : exemples…**
  - **Agent :** diffamation via terminal personnel hors des heures de travail
  - **EPES :** sécurisation insuffisante du SI →
    - ✓ exposition à des contenus illégaux, ou
    - ✓ dommage causé à l'ordinateur d'un visiteur, ou
    - ✓ destruction de résultats d'examen…
  - **EPES (voire agent pour une part) :** publication d'un site contrefaisant et injurieux grâce aux moyens fournis par l'établissement (Escotat vs Lucent, TGI Marseille 03 et CA Aix-en-Pvce 06)

Droits et obligations dans le cadre de la démarche de sécurisation (extraits)

Droits/obligations cadre démarche de sécurisation : extraits

- **Surveillance, journalisation et analyse... :**
  - **Opérateur** (EPES→ visiteurs, étudiants) **:**
    - ✓ Ppe d'anonymat… mais données de sécurité poss.
    - ✓ aucune analyse ou conservation des contenus
  - **Dans l'entreprise :** contrôle employeur de l'activité du personnel pendant le travail (→ agents)
    - ✓ Finalité : sécurité, contrôle de l'activité...
    - ✓ Transparence : consult. IRP, info. salariés, CNIL
    - ✓ Proportionnalité (dossiers/emails personnels)
  - **Dans toutes les situations :** droit des AR de voir les contenus personnels, + confidentialité

Droits/obligations cadre démarche de sécurisation : extraits

- **Filtrage ?**
  - **Opérateur :** obligation de neutralité (hors sécu réseau, intégrité services, accord)
  - **EPES :**
  - ✓ Sécurité des réseaux
  - ✓ Protection juridique (abonné, employeur)
  - ✓ En charge d'une MSP → contenus sans liens … mais attention entrave fct^{ment} services / attentes légitimes
- **En cas d'infraction … signalement ?**
  - Obligation des fonctionnaires (crimes /délits dans l'exercice fonctions) + obligation dénonciation 434-1 CP
  - Situations à risque sur le terrain de la complicité

Obligations tenant à la lutte contre les infractions et les contenus illicites

Obligations de conserver certaines données techniques

- **Opérateurs, FAI à titre « accessoire » : conserver les données relatives au trafic** (visiteurs, étudiants…) CPCE, D^{t} 06
  - **Principe d'anonymisation... mais obligation de conservation - 1 an** (sanction 1 an / 75 000 €)
  - **Finalités :** mise à disposition de l'**autorité jud. / Hadopi / agents habilités en mat. de lutte c/ le terrorisme** (certaines données uniquement) ; obligation d'établir « des procédures internes permettant de répondre aux demandes » (2011)
  - **Données techniques**, identités a priori non concernées ; traitements soumis à la loi de 78

Obligations de conserver certaines données techniques (suite)

- **FAI - Obligation de conserver les données d'identification** (LCEN / Décret 2011)
  - **Données techniques, autres infos seulement si collectées habituellement** (nom, prénom, adresses, tél, mot de passe...)
  - **Finalité :** communication sur réquisition de l'**autorité judiciaire** ; sur demande d'**agents habilités en matière de prévention du terrorisme**
  - Durée : 1 an – mêmes sanctions
  - Traitements soumis à la loi de 1978

Obligations de limiter certaines activités réseaux

- **Obligations de filtrage**
  - **Sur ordonnance du juge :**
    - ✓Opérateurs jeux ou paris en ligne non autorisés et n'ayant pas répondu à 1 injonction de l'ARJEL (L.2010)
    - ✓Atteinte à un droit d'auteur ou voisin, toute atteinte en ligne... (CPI Hadopi 1, LCEN, CPC)
  - **Notification de l'autorité administrative -** images pédopornographiques **(à venir – 03/2012)**

→ **Mais : concl. avocat général CJUE aff. SCARLET/SABAM :** la loi Belge autorisant le juge à ordonner le filtrage n'est pas conforme aux principes Conv. EDH

Obligations d'information et de mise en place de dispositifs de signalements ?

- **FAI :** information sur l'existence de moyens de filtrage (services Internet // moyens labellisés hadopi) ?
- **Opérateurs :** inform. sur les moyens de protection c/ les risques d'atteinte vie privée et sécu individuelle ? (O^{ce} 11)
- **Opérateurs :** information sur les conséquences de comportements illicites sur Internet ? (O^{ce} 2011)
- **FAI :** mise en place de dispositifs …
  - ➢ de signalement ? (LCEN : haine rac., pédopornographie…)
  - ➢ d'information ? (sur les sites de jeux en ligne tenus pour répréhensibles, les risques encourus en les utilisant)

Conclusion ?

- **Droits et obligations (plutôt) certains**
  - **Respect du RGS :**
    - ✓ échanges de l'AA, traitement, conservation ;
    - ✓ état de l'art (non respect peut entraîner 1 responsᵗ)
  - **Sécurité des DCP / secret** des correspondances
  - **Filtrage** sur demande du juge / de l'autorité admin.
  - **Conservation des données** d'identification/de trafic (étudiants, visiteurs)
  - **Droit de contrôle des employés**, avec ses limites
  - **Droit de préserver ses intérêts** : conserv. données pour raison de sécurité, filtrage (avec prudence : fonctionnement des services / attentes utilisateurs)…

Conclusion ?

- **Obligations (plutôt) incertaines**
  - ➢ Autres obligations FAI/opérateurs: d'info et de mise en place de dispositifs de signalement ; sécurité et intégrité des réseaux (même si intérêt + sécurité juridique + RGS)
  - ➢ Notification de violation de DP
  - ➢ Modalités de respect de l'obligation de sécuriser l'accès pour empêcher la contrefaçon (en l'absence de moyens labellisés ; si moyens incompatibles…)
  - → Difficultés partagées avec les entreprises, parfois les citoyens

Merci !

estelle.de.marco@inthemis.fr