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

Estelle De Marco
Inthemis
Espace Richter Center – 80 place Ernest Granier – 34000 Montpellier.

Résumé

Les établissements publics d'enseignement supérieur organisent l'accès à Internet ou à leur réseau local, de plusieurs catégories de personnes que sont en particulier leur personnel, leurs étudiants, ou des visiteurs occasionnels. Dans ce contexte, ils disposent de certains droits mais font également face à diverses obligations, récemment modifiées par le législateur et le pouvoir réglementaire (loi du 23 janvier 2006 relative à la lutte contre le terrorisme, lois dites Hadopi 1 et Hadopi 2 de 2009, loi du 12 mai 2010 sur les jeux d'argent en ligne, loi du 14 mars 2011 dite LOPPSI 2...). L'étude se propose de faire le point sur ces différents droits et obligations, en abordant dans un premier temps les droits et obligations de sécurisation du système d'information et de son utilisation (RGS, données à caractère personnel, obligation de vigilance contre la contrefaçon, enjeux de la sécurisation...), et dans un second temps les obligations tenant à la lutte contre les infractions et les contenus illicites (obligations de conserver les données relatives au trafic et d'identification, obligations de filtrage...).

Mots clefs

Enseignement supérieur ; accès aux réseaux informatiques ; droits, obligations et responsabilités des établissements publics ; sécurité des systèmes d'information ; sécurité des données à caractère personnel ; vigilance contre la contrefaçon ; surveillance et journalisation ; chartes ; filtrage ; conservation des données de trafic et d'identification ; lutte contre les contenus illicites.

Introduction*

Les établissements publics d'enseignement supérieur organisent l'accès à Internet ou à leur réseau local, de plusieurs catégories de personnes que sont en particulier leur personnel, leurs étudiants, ou des visiteurs occasionnels.

Dans ce cadre, ces établissements disposent de divers droits et obligations, notamment en leurs qualités d'établissement public chargé du service public de l'éducation, d'employeur, de titulaire d'un accès Internet, voire de fournisseur d'accès à Internet.

Cette multiplicité de qualités entraîne des droits et obligations qui peuvent s'avérer divergents, voire contradictoires, lorsqu'ils ne sont pas incertains. A ces problématiques s'ajoutent de récentes modifications législatives et réglementaires, notamment apportées par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, les lois dites Hadopi 1 et Hadopi 2 de 2009, la loi du 12 mai 2010 sur les jeux d'argent en ligne, et la loi du 14 mars 2011 dite LOPPSI 2.

La présente étude se propose de dresser le panorama des principaux droits et obligations des établissements publics d'enseignement supérieur, en se concentrant sur les dernières modifications qui leur ont été apportées. A cette fin, après avoir analysé en quoi les établissements publics d'enseignement supérieur pouvaient être assimilés à la catégorie des fournisseurs d'accès à Internet (1), nous aborderons les droits et obligations de sécurisation du système d'information et de son utilisation (2), avant de nous intéresser aux obligations tenant à la lutte contre les infractions et les contenus illicites (3).

1 Les établissements publics d'enseignement supérieur, fournisseurs d'accès à Internet ?

Les établissements publics d'enseignement supérieur sont chargés du service public de l'éducation, et ont la qualité d'employeur vis-à-vis de leur personnel. Ils ont encore signé une convention d'agrément voire une convention financière[1] avec le fournisseur d'accès à Internet Renater, ce qui les fait entrer dans la catégorie des « abonnés » à Internet[2], dans le cadre de l'application de certaines dispositions de la loi. L'ensemble de ces « casquettes » entraînent des droits et des obligations différents.

Une question est toutefois de savoir si ces établissements doivent également être considérés comme des fournisseurs d'accès à Internet (FAI), lorsqu'ils organisent l'accès de leur personnel, de leurs étudiants ou de visiteurs à leur réseau local ou à Internet, ce qui impliquerait l'application de droits et d'obligations complémentaires.

*Avertissement : le présent article reflète uniquement l'opinion de son auteur ; il n'a pas valeur de consultation juridique.

[1]Voir la page dédiée aux agréments sur le site de Renater, à l'adresse http://www.renater.fr/spip.php?rubrique6.

[2]Le terme d' « abonné » est défini comme étant « *toute personne physique ou morale partie à un contrat avec un fournisseur de services de communications électroniques accessibles au public, pour la fourniture de tels services* », par l'article 2, k de la directive 2002/21/CE du 7 mars 2002, accessible à l'adresse http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:FR:HTML (directive modifiée par la directive 2009/140/CE du 25 novembre 2009).

La Cour d'appel de Paris, en 2005[3], a répondu de manière positive à cette question, en assimilant une entreprise à un FAI[4], lorsque cette dernière permet l'accès à Internet depuis ses postes informatiques. Les juges, dans cette décision qui est transposable aux établissements publics d'enseignement supérieur, considèrent que l'entreprise doit par conséquent respecter l'obligation faite aux FAI de conserver les données d'identification de leurs utilisateurs[5]. Ils ne donnent toutefois aucune précision sur l'application des autres obligations prévues notamment par la loi du 21 juin 2004 pour la confiance dans l'économie numérique[6].

L'article L. 34-1 du code des postes et des communications électroniques (CPCE), qui pose une obligation de conservation des données de trafic distincte de celle que nous venons d'évoquer, assimile par ailleurs les FAI à la catégorie des opérateurs[7]. Il ne précise toutefois pas si cette assimilation ne vaut que pour ses propres dispositions, ou si elle vaut pour l'ensemble du code : on pourrait le penser au vu de la formule générale qu'il emploie[8], mais l'ensemble des obligations applicables aux opérateurs ne sont pas toujours adaptées à la simple fourniture d'accès[9], a fortiori si les entreprises et par extension les établissements publics d'enseignement supérieur devaient être inclus dans cette dernière catégorie.

Ce code semble ceci dit préciser, contrairement à ce que dit la Cour d'appel de Paris, que les structures dont l'activité de fourniture d'accès n'intervient qu'en « accessoire » à une autre activité, tels que les entreprises ou les établissements publics d'enseignement supérieur, ne sont pas des FAI. Il énonce en effet, depuis la loi du 23 janvier 2006[10], que *« les 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, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article* ». Soumettre ces fournisseurs d'accès « à titre accessoire » au respect de ces dispositions particulières revient en effet à dire que par opposition, les autres dispositions du code ne leur sont pas applicables. Malgré tout, les FAI « traditionnel » étant définis de la même manière dans la LCEN et dans le CPCE, il ne reste pas totalement exclu que l'analyse de l'arrêt précité de la Cour d'appel de Paris soit à l'avenir transposée à certaines dispositions du CPCE.

La conclusion que nous pouvons tirer de ce contexte juridique assez obscur est que les dispositions de l'article L. 34-1 du CPCE, concernant les droits et obligations des opérateurs en matière de conservation des données de trafic, sont explicitement applicables aux établissements publics d'enseignement supérieur, au moins lorsque ces derniers offrent un accès à Internet à des personnes pouvant être qualifiées de « public »[11], notion qui s'applique très certainement aux étudiants et visiteurs[12]. Selon la Cour d'appel de Paris, l'obligation de conservation des données d'identification mise à la charge des FAI par l'article 6 de la loi du 21 juin 2004 est également applicable aux entreprises, et par extension aux établissements publics d'enseignement supérieur. S'agissant des autres dispositions applicables aux opérateurs et aux fournisseurs d'accès, un doute subsiste et il s'agira d'apprécier dans chaque hypothèse la pertinence de leur application.

---

[3] Cour d'appel de Paris, 14ème chambre, section B, 4 février 2005, SA BNP Paribas vs Société World Press Online, http://www.droit-tic.com/juris/aff.php?id_juris=17.

[4] La Cour considère qu'une entreprise est un « *prestataire technique au sens de l'article 43-7 de la loi du 1er août 2000 »,* renvoyant en réalité à l'article 43-7 de la loi n° 86-1067 du 30 septembre 1986 tel que modifié par l'article 1 de la loi n° 2000-719 du 1er août 2000. Cet article 43-7 faisait référence aux « *personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée* », autrement dit aux FAI tels qu'on les désigne habituellement. Il a été abrogé et remplacé par l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, qui fait référence aux « « *personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* », formule un peu différente mais désignant les mêmes acteurs.

[5] Voir infra notre sous-titre 3.1.

[6] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Sur ces autres obligations, voir notamment notre sous-titre 3.3.

[7] L'article L. 32 du CPCE définit les opérateurs comme les personnes « *exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* ». Cette notion de « fourniture de service de communications électroniques » est entendue comme étant une activité de « *transport de communications* » (Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, Montpellier 1, 2005, ANRT (ISBN : 978-2-7295-6899-3 ; Réf. : 05MON10067), n° 266 et suivants), ou de « *transmission de signaux* » (directive 2002/21/CE, dite « directive « cadre », que le CPCE transpose) sur les réseaux.

[8] L'article L. 34-1 du CPCE commence en effet en ces termes : « « *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne…* ».

[9] En 2004, l'ARCEP distinguait clairement les activités de FAI et celles d'opérateur. Elle précisait sur son site web que le FAI « *peut choisir d'utiliser les services d'un opérateur de transport de données, afin que son service d'accès à Internet soit rendu accessible depuis l'ensemble des zones géographiques couvertes par ce transporteur. Dans ce cas, le réseau de transport de données relie le réseau de télécommunications local au fournisseur d'accès Internet. Il est constitué d'un ensemble de liaisons et équipé de passerelles d'une technologie adaptée à la norme de transmission sur Internet, (la norme IP) »*. L'ARCEP précisait par ailleurs que le « *fournisseur d'accès à Internet gère les abonnements à Internet de ses clients et effectue la liaison avec un point d'échange de données d'Internet. Cette liaison peut être sous-traitée à un transporteur de données* », la notion de « transporteur » de données visant dans la loi l'opérateur (voir supra, note n°7).

[10] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JORF n° 20 du 24 janvier 2006 p. 1129, texte n° 1, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053177.

[11] La jurisprudence considère que les membres d'un groupement privé doivent être « *liés par une communauté d'intérêts* », et il suffit qu'une information touche une personne extérieure à ce groupement pour que cette information devienne « publique » (ex. Cour de cassation, ch. criminelle, 18 mai 1954 ; TGI Paris, 25 oct. 1999). Le TGI de Paris, dans sa décision précitée, précise que la notion de « *communauté d'intérêts suppose certaines conditions d'admission au groupement* », quelles qu'elles soient, « le *simple assemblage inorganisé d'individus attirés par une passion commune* » étant insuffisant, puisque « *l'accès du public à ce groupement informel (demeure) entièrement libre et spontané* ». Ces décisions, transposées à notre problématique, conduisent à dire que l'accès offert aux visiteurs est un accès offert au « public ». La question est plus délicate pour les étudiants, mais l'accès qui leur est offert est généralement offert également à d'autres personnes (étudiants d'autres établissements, visiteurs...), ce qui semble a priori suffire pour entraîner la notion de « public ».

[12] La réponse est moins claire s'agissant des employés. La Cour d'appel de Paris ne précise pas dans son arrêt si les postes informatiques en cause ne permettaient l'accès qu'aux employés ou à des personnes tierces. Sur ce point, voir infra notre sous-titre 3.1.

2 Les droits et obligations des établissements publics d'enseignement supérieur en matière de sécurisation du système d'information et de son utilisation

Aux obligations de sécurisation du système d'information et de son utilisation (2.1), s'ajoute un droit de sécuriser le système d'information et son utilisation (2.2), qui permet aux établissements publics d'enseignement supérieur de faire face à plusieurs enjeux, notamment en termes de responsabilité. Ces établissements ont encore des droits et obligations dans le cadre de la démarche même de sécurisation (2.3).

2.1 Les obligations de sécurisation du système d'information et de son utilisation

Les obligations de sécurisation attachées au système d'information ou à son utilisation peuvent être classées en deux catégories. Aux côtés des obligations de sécurisation attachées à la personne (3.1.1), existent des obligations de sécurisation des données en raison de leur nature (3.1.2).

2.1.1 Les obligations de sécurisation du système d'information attachées à la personne

Parmi ces obligations figurent notamment l'obligation des autorités administratives de respecter le référentiel général de sécurité (2.1.1.1) et les obligations des FAI en termes de sécurisation des réseaux et des communications (2.1.1.2).

2.1.1.1 L'obligation des autorités administratives de respecter le référentiel général de sécurité (RGS)

Le référentiel général de sécurité (RGS) est prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005[13], ses conditions d'élaboration, d'approbation, de modification et de publication étant fixées par le décret n° 2010-112 du 2 février 2010[14]. Sa version 1.0 du 6 mai 2010[15] a été approuvée par arrêté du 6 mai 2010[16].

Le RGS « *fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées* »[17] par voie électronique. Il n'est donc impératif que pour les autorités administratives et les prestataires qui les assistent dans leur démarche de sécurisation, et uniquement pour ce qui concerne les échanges par voie électronique entre les autorités administratives et les usagers, et entre autorités administratives. Il est applicable aux établissements publics d'enseignement supérieur[18], lorsque ces derniers sont susceptibles d'échanger des informations électroniques avec des usagers ou d'autres autorités administratives[19].

L'article 14, I de l'ordonnance de 2005 prévoit par ailleurs que les systèmes d'information existants à la date de publication du RGS doivent être mis en conformité avec celui-ci dans un délai de trois ans à compter de cette date, et que les applications crées dans les six mois suivant la date de publication du référentiel doivent être mises en conformité avec celui-ci au plus tard 12 mois après cette date.

L'ordonnance de 2005 ne s'applique pas, en revanche, aux systèmes d'information relevant du secret de la défense nationale, qui font l'objet de dispositions spécifiques[20].

S'agissant du contenu de l'obligation, l'article 3 du décret de février 2010 impose aux autorités administratives, et donc aux établissements publics d'enseignement supérieur, dans les conditions fixées par le RGS :

- D'identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;
- De fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés[21] ;
- D'en déduire des fonctions de sécurité (authentification, signature électronique, confidentialité, horodatage...), ainsi que le niveau de ces fonctions permettant d'atteindre ces objectifs ;

[13]Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=AB10CD76BB11A5013046CF86D0EEDF3D.tpdjo10v_2&dateTexte=?cidTexte=JORFTEXT000000636232&categorieLien=cid, art. 9.

[14]Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 , disponible sur le site de Légifrance : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=&categorieLien=id#.

[15]La version 1.0 du RGS peut être trouvée sur le site web de l'ANSSI à l'adresse suivante : http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/.

[16]Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000022220429&dateTexte=&oldAction=rechJO&categorieLien=id.

[17]Article 1 du décret n° 2010-112.

[18]La notion d'autorité administrative inclut les « *organismes chargés de la gestion d'un service public administratif* » (article 1 de l'ordonnance).

[19]RGS, p. 6.

[20]Article 15 de l'ordonnance. Voir infra notre sous-titre 2.1.2.

[21]Voir pour plus de précisions la p.10 du RGS.

- De respecter les règles correspondantes formulées dans le RGS, sachant que les produits de sécurité et services de confiance utilisés peuvent faire l'objet d'une qualification[22];
- De réexaminer régulièrement la sécurité du système et des informations en fonction de l'évolution des risques, dans les conditions fixées par le RGS.

Préalablement à toute mise en service opérationnelle du système d'information, ce dernier doit en outre faire l'objet d'une « homologation de sécurité »[23], rendue accessible aux utilisateurs du système[24], et « *régulièrement réexaminée, afin de prendre les mesures que peuvent imposer les évolutions du système, de ses composants, de son emploi, du contexte humain ou organisationnel, ou (…) de la menace* »[25]. Prononcée par une « autorité d'homologation » désignée par l'établissement, habituellement au sein de ce dernier[26], cette homologation est un engagement par lequel l'autorité d'homologation atteste, au nom de l'établissement, « *que le projet a bien pris en compte les contraintes opérationnelles de sécurité établies au départ, que les exigences de sécurité sont bien déterminées et satisfaites, que les risques résiduels sont maîtrisés et acceptés, et que le système d'information est donc apte à entrer en service* »[27]. Afin que la décision de l'autorité d'homologation soit motivée et justifiée, le RGS recommande que cette autorité « *s'appuie sur un dossier de sécurité constitué selon le modèle décrit dans le guide GISSIP* »[28]. Ce dernier guide préconise par ailleurs, entre autres mesures, que l'homologation soit faite conformément à une note d'orientation SSI[29], et que l'autorité d'homologation s'appuie sur une « commission d'homologation » qui l'assistera « afin de lui fournir les éléments nécessaires à sa décision »[30], et dans le cadre duquel sera prise la décision d'homologation[31].

2.1.1.2 Les obligations des opérateurs en termes de sécurité des réseaux et des communications

Les opérateurs ont l'obligation, aux termes de plusieurs articles du code des postes et des communications électroniques, d'assurer la sécurité de leurs réseaux et des communications sur ces réseaux.

Plus précisément, ils doivent assurer le secret des correspondances, la neutralité et l'intégrité des messages transmis sur leurs réseaux, et porter à la connaissance de leur personnel les obligations et peines qu'il encourt au titre des dispositions du code pénal, dont celles relatives au secret des correspondances et au secret professionnel[32].

Il doivent également assurer l'intégrité et la sécurité de leurs réseaux quand ceux-ci sont ouverts au public[33]. Depuis l'ordonnance n°2011-1012 du 24 août 2011[34], le ministre chargé des communications électroniques peut par ailleurs imposer « *à tout opérateur de soumettre ses installations, réseaux ou services à un contrôle de leur sécurité et de leur intégrité »,* effectué *« par un service de l'État ou un organisme qualifié indépendant »* désigné par ce ministre, et *« de lui en communiquer les résultats ».* A cette fin, l'opérateur doit fournir « *au service de l'État ou à l'organisme chargé du contrôle toutes les informations et l'accès à ses équipements, nécessaires pour évaluer la sécurité et l'intégrité de ses services et réseaux, y compris les documents relatifs à ses politiques de sécurité* », le coût du contrôle étant « *à la charge de l'opérateur* »[35].

---

[22]Voir notamment l'art. 4 de l'ordonnance et son chapitre III.

[23]Cette obligation d'homologation est posée à l'art. 5 du décret n°2010-112 : « *L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3* ». Cette « attestation formelle » correspond selon le RGS à une « décision d'homologation ».

[24]Le décret ne précise pas les modalités de cette mise à disposition. Il se contente de dire (par renvoi à l'ordonnance de 2005) que dans le cas d'un téléservice, la décision « est rendue accessible aux usagers » depuis ce service (article 5 du décret).

[25]RGS p. 13.

[26]Voir le RGS, p. 13. La composition de cette autorité n'est pas réglementée, mais il peut s'agir d'une seule personne (voir RGS p. 30). Le RGS précise (p. 13) que lorsque le système est sous la responsabilité de plusieurs autorités administratives, l'autorité d'homologation est désignée conjointement par ces dernières.

[27]RGS p. 13.

[28]Le GISSIP, Guide d'intégration de la sécurité des systèmes d'information dans les projets, est accessible à l'adresse suivante : http://www.ssi.gouv.fr/IMG/pdf/GISSIP-Methode-2006-12-11.pdf.

[29]Note permettant de définir la stratégie de sécurité à adopter en précisant les enjeux du projet, devant être validé par l'autorité d'homologation dès l'étude d'opportunité : voir GISSIP, p. 9.

[30]GISSIP, p. 9.

[31]Voir page 11 du GISSIP. La décision peut être une homologation provisoire, une homologation définitive pour une durée recommandée de 3 à 5 ans, ou un refus d'homologation (voir p. 14 du RGS et p. 11 du GISSIP).

[32]Article D. 98-5, I (renvoyant aux articles 226-13, 226-15, 432-9 du code pénal). Voir aussi les articles L. 32-1, L. 33-1 (depuis l'ordonnance n°2011-1012 du 24 août 2011, http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&categorieLien=id) et D.98-5, III (selon lequel les opérateurs doivent prendre « *toutes les dispositions nécessaires pour assurer la sécurité des communications* » empruntant leur réseau, et informer leurs abonnés des éventuels services permettant de renforcer la sécurité des communications, ainsi que des risques particuliers de violation de la sécurité du réseaux et des moyens d'y remédier, lorsqu'un tel risque existe).

[33] Article L. 32-1 et, depuis l'ordonnance n°2011-1012 du 24 août 2011 (précitée), article L. 33-1 du CPCE. Selon ce dernier article et l'article D. 98-4 du CPCE, les réseaux doivent encore répondre à des conditions de permanence, de qualité, et de disponibilité.

[34]Ordonnance 2011-1012 du 24 août 2011 relative aux communications électroniques, JORF n°0197 du 26 août 2011 page 14473, art. 38, accessible sur le site de Legifrance à l'adresse : http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&categorieLien=id.

[35]Nouvel article L. 33-10 du CPCE.

Nous avons vu[36] que l'application de ces obligations aux établissements publics d'enseignement supérieur reste très incertaine. Toutefois, les dispositions relatives à la protection de la vie privée et des correspondances ne sont en définitive que la transcription de règles s'appliquant de manière plus générale à toute personne et particulièrement à celles qui sont en charge d'une mission de service public[37], que les établissements publics d'enseignement supérieur doivent également respecter. Concernant l'obligation d'assurer l'intégrité et la sécurité de leurs réseaux, il convient de noter que ces établissements ont un intérêt particulier à la mettre en œuvre, compte tenu de leurs missions. Une telle mise en œuvre sera dès lors de nature à renforcer leur sécurité juridique en cas de mise en cause sur la base de ces dispositions.

2.1.2 Les obligations de sécurisation du système d'information selon la nature des données

Les établissements publics d'enseignement supérieur ont également à leur charge diverses obligations de sécurisation tenant à la nature de certaines données. Il s'agit par exemple des obligations de sécurité à respecter en matière de secret de la défense nationale[38], d'obligations contractuelles (accord de confidentialité, convention de preuve...)[39], ou d'obligations tenant à la conservation et à l'archivage[40], impliquant que les informations concernées soient sécurisées pour notamment préserver leur intégrité, disponibilité et intelligibilité. Nous analyserons plus précisément deux de ces obligations, que sont l'obligation de sécurisation des données à caractère personnel (2.1.2.1) et l'obligation de sécurisation contre la contrefaçon (2.1.2.2).

2.1.2.1 L'obligation de sécurisation des données à caractère personnel

En premier lieu, comme tout responsable de traitement de données à caractère personnel, les établissements publics d'enseignement supérieur ont l'obligation 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 ne soient déformées, endommagées, ou que des tiers non autorisés y aient accès* », selon l'article 34 de la loi du 6 janvier 1978[41]. Le non-respect de cette obligation est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-17 du code pénal).

Par ailleurs, l'article 34 bis de la loi de 1978, créé par l'article 38 de l'ordonnance 2011-1012 du 24 août 2011[42], impose aux « *fournisseurs de services de communications électroniques* », donc aux opérateurs, sous peine des mêmes sanctions, d'avertir sans délai la Commission nationale de l'informatique et des libertés (CNIL) de toute violation de données à caractère personnel, autrement dit de « *toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* ». « *Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique* », le fournisseur doit encore en avertir l'intéressé sans délai, sauf si la CNIL constate que le fournisseur avait mis en œuvre « *des mesures de protection appropriées (…) afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès* », et que ces mesures avaient été appliquées aux données concernées par la violation. Enfin, un inventaire des violations de données à caractère personnel doit être tenu par l'opérateur, précisant notamment leurs modalités, leur effet et les mesures prises pour y remédier, et doit être conservé à la disposition de la CNIL.

[36]Voir supra, notre titre 2.

[37]Les articles 226-15 et 432-9 du code pénal répriment l'interception de correspondances, l'article 432-9 la réprimant plus sévèrement lorsque l'auteur est un opérateur ou une personne chargée d'une mission de service public. L'article 9 du code civil protège par ailleurs plus largement la vie privée. Pour ce qui concerne l'information du personnel en ce qui concerne les sanctions qu'il encourt, elle est par ailleurs vivement conseillée, comme nous le verrons infra, 2.3.

[38]L'arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale (JORF n°0184 du 11/08/10 p. 14718, texte n°1, accessible à l'adresse http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E607348D4A049DC1032EB2BFA17BBFAA.tpdjo10v_2?cidTexte=JORFTEXT000022683377&categorieLien=id) définit notamment les règles à respecter pour la protection des informations classifiées secret défense et les systèmes d'information qui interviennent dans leur traitement. Il concerne « *toutes les entités, publiques ou privées, concernés par le secret de la défense nationale, ainsi (que) toute personne dépositaire, même à titre provisoire, d'un tel secret, y compris dans le cadre de la passation et de l'exécution d'un contrat* » (art. 3). Plusieurs comportements considérés comme constituant des atteintes au secret de la défense nationale sont réprimés par les art. 413-10 et suivants du code pénal.

[39]Les obligations contractuelles s'imposent aux parties : voir les articles 1134 et 1135 du code civil, et, en matière de contrat de droit public, la décision du Conseil d'État du 30 mars 1916 (disponible aux adresses : http://legimobile.fr/fr/jp/a/ce/ad/1916/3/30/59928/ ; http://lexinter.net/JPTXT2/arret_gaz_de_bordeaux.htm) selon laquelle « *en principe, le contrat de concession règle d'une façon définitive jusqu'à son expiration, les obligations respectives du concessionnaire et du concédant* », affirmation considérée par la doctrine comme s'appliquant à l'administration et à son cocontractant dans le cadre de tous les contrats administratifs (voir par exemple « Principes fondamentaux relatifs à l'exécution du contrat administratif », Jurispedia, http://fr.jurispedia.org/index.php/Principes_fondamentaux_relatifs_%C3%A0_l%27ex%C3%A9cution_du_contrat_administratif_%28fr%29). En cas d'inexécution d'une obligation contractuelle, la partie fautive pourra avoir à réparer le préjudice qu'elle aura causé à son cocontractant.

[40]Aux termes de l'art. L. 211-4 du code de l'éducation, tous « *les documents qui procèdent de l'activité, dans le cadre de leur mission de service public, (…) des (…) personnes morales de droit public (...)* » sont des archives publiques. Elles doivent être conservées dans les conditions précisées par le code du patrimoine.

[41]Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978 page 227, disponible à l'adresse http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20080609, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JORF du 7 août 2004, p.14063, texte n°2, disponible à l'adresse http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=3ED775F730CEE1C0B1B0C9BE95F1796B.tpdjo11v_2?cidTexte=JORFTEXT000000441676&categorieLien=id.

[42]Ordonnance 2011-1012 du 24 août 2011 relative aux communications électroniques, précitée en note 34. Elle transpose sur ce point la directive 2009/136/CE du Parlement et du Conseil du 25 novembre 2009, qui modifie notamment la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO n° L 337 du 18/12/2009, p. 0011-0036, accessible à l'adresse http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:FR:HTML).

Le I de cet article 34 bis précise que ces dispositions sont applicables aux traitements « *mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification* ». Comme nous l'avons vu, cela signifie qu'elles sont applicables aux seuls opérateurs. Leur application aux FAI « à titre accessoire » que sont les établissements publics est donc incertaine, compte tenu de leur imparfaite assimilation à la catégorie des FAI, et de l'incertitude de l'assimilation systématique de ces derniers à la catégorie des opérateurs[43]. Ceci dit, étant donné que ces établissements ont à leur charge une obligation de conservation de certaines données de trafic et d'identification[44], que cette obligation est mise à leur charge en leur qualité de FAI pour ce qui concerne les données d'identification, et que cette conservation est expressément visée par l'article 34-1, envisager de la respecter pourrait sembler judicieux[45].

Il convient par ailleurs de noter l'existence d'une proposition de loi, pour l'heure adoptée uniquement par le Sénat le 23 mars 2010[46], qui prévoit de mettre une obligation similaire à la charge de tous les responsables de traitement de données à caractère personnel. Les différences entre ce texte et l'article 34 bis résident dans l'obligation de notifier la violation à la personne intéressée en tout état de cause, sauf lorsque le traitement est autorisé en vertu des dispositions de la l'article 26 de la loi de 1978[47], dans la possibilité de notifier la violation au correspondant informatique et liberté (CIL) lorsqu'il existe et non à la CNIL, et dans l'obligation de prendre immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données, ce dont le CIL doit informer la CNIL. Selon ce texte, l'inventaire des violations doit par ailleurs être tenu à jour par le CIL.

2.1.2.2 L'obligation de sécurisation contre la contrefaçon

L'article L. 336-3 du code de la propriété intellectuelle (CPI)[48] pose une obligation de vigilance à la charge des personnes titulaires d'un accès à des services de communication au public en ligne. Selon ses termes, ces personnes, qui peuvent être physiques ou morales et qui incluent donc les établissements publics d'enseignement supérieur, ont « *l'obligation de veiller à ce que (leur) accès ne fasse pas l'objet d'une utilisation* » à des fins de contrefaçon[49].

L'article R. 335-5 du CPI, créé par le décret du 25 juin 2010[50], institue quant-à-lui une contravention de négligence caractérisée. Selon ses termes, constitue une négligence caractérisée « *le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne (…) »,* soit *« de ne pas avoir mis en place un moyen de sécurisation de cet accès »,* soit *« d'avoir manqué de diligence dans la mise en œuvre de ce moyen »,* lorsque cette personne a reçu de la part de la commission de protection des droits (CPD) de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (dite HADOPI) une recommandation de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir une nouvelle utilisation de celui-ci à des fins de contrefaçon, et que, dans l'année suivant la présentation de cette recommandation, cet accès a de nouveau été utilisé à des fins de contrefaçon.

En d'autres termes, pour que cette contravention soit applicable, il faut que l'établissement public ait reçu une recommandation de la CPD de l'HADOPI lui enjoignant de mettre en œuvre un moyen de sécurisation, et que dans l'année suivant cette recommandation l'accès à Internet de cet établissement ait à nouveau été utilisé à des fins de contrefaçon, alors qu'il n'avait pas mis en œuvre un tel moyen ou qu'il ne l'avait pas fait avec toutes les diligences nécessaires. Concernant ces moyens de sécurisation, il est prévu que l'HADOPI publie une liste de moyens labellisés, répondant à une série de spécifications fonctionnelles déterminées et rendues publiques par elle, cette labellisation devant être périodiquement revue[51].

Pour que cette contravention soit appliquée, il faut encore que l'HADOPI saisisse le juge de l'ordre judiciaire, qui devra se prononcer sur la question savoir si la mise en œuvre d'un logiciel de sécurisation non labellisé peut-être de nature à exonérer l'établissement

[43]Voir supra, notre titre 1.

[44]Voir supra, notre titre 1, et infra, notre sous-titre 3.1.

[45]Le non respect de cette obligation est passible de cinq ans d'emprisonnement et de 300 000 euros d'amende (226-17-1 du code pénal).

[46]Proposition de loi adoptée par le Sénat visant à mieux garantir le droit à la vie privée à l'heure du numérique, adoptée le 23 mars 2010. Ce texte est disponible à l'adresse http://www.senat.fr/leg/tas09-081.html. Son dossier législatif est disponible à l'adresse http://www.senat.fr/dossier-legislatif/ppl09-093.html.

[47]Cet article est relatif aux traitements de données à caractère personnel mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense ou la sécurité publique, ou ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

[48]Cet article a été introduit par l'article 11 de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9971EAB038D4B632A648FA5EC4205E96.tpdjo10v_2?cidTexte=JORFTEXT000020735432&dateTexte=20090614. Il remplace ceci dit l'ancien article L. 335-12 du CPI, qui depuis la loi dite DADVSI du 1er août 2006 prévoyait une obligation dont les termes étaient assez proches.

[49]L'article évoque plus exactement « *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* ».

[50]Décret n°2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur Internet, JORF n° 0146 du 26 juin 2010 page 11536, accessible à l'adresse http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9971EAB038D4B632A648FA5EC4205E96.tpdjo10v_2?cidTexte=JORFTEXT000022392027&categorieLien=id.

[51]Article 331-26 du CPI. Cette liste sera établie au terme d'une procédure d'évaluation et de labellisation fixée par les articles R. 331-85 et suivants du CPI, articles créés par le décret 2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne (accessible sur Légifrance à l'adresse http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023295302&categorieLien=id).

de sa responsabilité, et sur ce qu'il convient d'entendre par un « manque de diligences » dans la mise en œuvre d'un moyen de sécurisation, deux points qui restent particulièrement obscurs. S'il est déclaré responsable de cette contravention, l'établissement pourra alors être condamné de l'amende prévue pour les contraventions de la cinquième classe[52], ainsi qu'à une « *peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois* », assortie d'une interdiction de souscrire un autre contrat sur cette période, sous peine de 3750€ amende, sachant qu'il conservera à sa charge le coût de l'abonnement ou de sa résiliation[53]. Le juge restera toutefois libre de ne pas appliquer cette sanction complémentaire, notamment s'il la trouve disproportionnée eu égard à l'infraction commise et compte tenu des missions de l'établissement.

Il convient de noter que la peine de suspension est également une peine complémentaire pouvant être prononcée en cas de contrefaçon, pour une durée maximale d'un an, aux termes de l'article L. 335-7. Le versement du prix de l'abonnement ou les frais d'une éventuelle résiliation resteront également, dans cette hypothèse, supportés par le titulaire de l'accès.

2.2 Le droit de sécuriser le système d'information

A côté des obligations de sécurisation, il existe un droit de sécuriser le système d'information et son utilisation, dont il convient de rechercher le fondement précis afin d'en mesurer l'étendue (2.2.1). Ce droit de sécuriser répond à différents enjeux (2.2.2).

2.2.1 Le fondement du droit de sécuriser le système d'information

A défaut d'obligation de sécuriser le système d'information et son utilisation, cette sécurisation est un droit, que l'on peut fonder de deux manières différentes s'agissant des établissements publics d'enseignement supérieur. En premier lieu, cette sécurisation peut être vue comme l'un des moyens leur permettant d'exercer les missions qui leur sont confiées par la loi, le code de l'éducation leur reconnaissant une autonomie d'administration[54]. En second lieu, il est possible de considérer que ces établissements bénéficient d'un droit de sécuriser au titre de leur droit de protéger leurs intérêts légitimes et du principe de « liberté »[55] posé par l'article 4 de la Déclaration des droits de l'Homme et du citoyen (DDHC)[56], voire au titre d'une liberté « nommée » comme le droit de propriété[57], puisque la sécurisation du système d'information a vocation à protéger certains autres droits, dans notre exemple les droits de propriété sur certaines informations voire le parc informatique.

Dans tous les cas, l'exercice de ce droit a des limites : le nécessaire respect des droits et libertés des tiers. Les autorités publiques ont en effet l'obligation d'assurer le respect des droits et libertés des citoyens. Toute limitation de ces droits doit, en plus d'être permise par la loi, poursuivre un but légitime, être nécessaire et adaptée à la réalisation de cet objectif, et lui être proportionnée, ceci résultant tant des principes posés par la Convention européenne des droits de l'Homme (Conv. EDH)[58] que de l'article 52 de la charte européenne des droits fondamentaux[59]. L'exercice de la liberté déclarée à l'article 4 de la DDHC doit avoir pour bornes, quant-à-elle, les règles définies par la loi, qui assurent aux tiers la jouissance de leurs propres droits[60]. Enfin, l'exercice d'une liberté « nommée » comme le droit de propriété doit généralement[61] être concilié avec la liberté des autres personnes[62], cette conciliation devant se faire selon les principes posés par la Conv. EDH énoncés plus haut.

En conséquence, les établissements publics d'enseignement supérieur doivent de manière générale veiller, lorsque les mesures de sécurité qu'ils mettent en place sont susceptibles de limiter les droits d'autres personnes, telles que leurs étudiants ou leur personnel, de prendre certaines précautions afin que ces limitations ne soient pas considérées comme illégitimes (une mesure de

[52]L'amende de la cinquième classe est de 1500 euros (article 131-13 du code pénal).

[53]Article L. 335-7-1 du CPI.

[54]Article L. 711-1 du code de l 'éducation.

[55]Traditionnellement, les droits et libertés accordées aux personnes physiques ne bénéficient pas aux personnes morales de droit public, comme les établissements publics d'enseignement supérieur. Ceci dit, ces établissements ont un statut particulier, notamment depuis la loi n° 2007-1199 du 10 août 2007 relative aux « libertés et responsabilités » des universités, susceptible de leur faire bénéficier de certains droits applicables aux personnes physiques, ce que la jurisprudence a parfois reconnu (voir en ce sens Emmanuel Decaux, « *L'applicabilité des normes relatives aux droits de l'homme aux personnes morales de droit privé* », Revue Internationale de Droit Comparé, 2-2002, p. 551-552., au sujet des collectivités locales).

[56]Cette Déclaration du 26 août 1789 relève du « bloc de constitutionnalité » selon les préambules de la Constitution du 27 oct. 1946 et de celle du 4 oct. 1958.

[57]Le droit de propriété a déjà été reconnu à une personne morale de droit public par le Conseil constitutionnel (décision 86-207 DC des 25-26 juin 1986). Voir également, Emmanuel Decaux, « *L'applicabilité des normes relatives aux droits de l'homme aux personnes morales de droit privé* », R.I.D.C., 2-2002, p. 552.

[58]Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950, disponible sur le site web du Conseil de l'Europe (http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=005&CM=&DF=&CL=FRE). Voir E. De Marco, *L'anonymat sur Internet et le droit*, cit. en note 7, n° 86.

[59] Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, accessible sur le site web du Parlement européen (http://www.europarl.europa.eu/charter/pdf/text_fr.pdf).

[60]« *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi* ».

[61]Les libertés pouvant être limitées selon ces principes sont des libertés dites « conditionnelles ». D'autres libertés ont un statut différent, comme par exemple le droit à la vie ou le droit de ne pas être soumis à la torture.

[62]Les principes de la Conv. EDH, applicables en premier lieu dans les rapports entre l'État et les particuliers, sont également considérés par la doctrine comme applicables dans les rapports entre particuliers : voir par exemple Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3ème éd., 1995, pp. 76-81.

sécurisation ayant pour but d'empêcher les agents publics d'exercer leur droit syndical serait par exemple sans aucun doute jugée illégitime) ou excessives (le contrôle du poste d'un employé est par exemple soumis à certaines limites, que nous verrons plus loin[63]), en tenant compte des dispositions de la loi et des décisions de justice déjà rendues en la matière, lorsqu'elles existent.

2.2.2 Les enjeux de la sécurisation du système d'information

Les enjeux de sécurisation du système d'information et de son utilisation sont multiples, mais peuvent pour l'essentiel être classés en deux catégories.

Il s'agit en premier lieu de protéger les intérêts particuliers de l'établissement. Ces intérêts recouvrent notamment la confiance des tiers[64], l'image de l'établissement et de son personnel[65], et le patrimoine de l'établissement, dans sa dimension matérielle (postes, réseaux, applications...) comme immatérielle (informations stratégiques, résultats de recherche, données administratives, actes juridiques...). Une interception de communications entre un membre du personnel de l'établissement et le réseau local peut par exemple conduire à l'accès illégitime d'un tiers à une information confidentielle. L'exploitation d'une faille par un visiteur peut encore permettre à celui-ci de s'introduire dans le système d'information et d'accéder à des informations stratégiques ou confidentielles, voire d'altérer un acte juridique, ainsi que sa validité ou sa force probante.

Il s'agit en deuxième lieu de renforcer la sécurité juridique de l'établissement et de son personnel. En effet, un établissement public d'enseignement supérieur ou un agent est notamment susceptible d'engager sa responsabilité dans plusieurs hypothèses : lorsqu'il méconnaît une obligation de sécurisation, telles celle que nous avons abordées dans notre 2.1, ou lorsqu'il commet une infraction ou méconnaît une autre obligation faisant l'objet d'une disposition légale ou réglementaire. Un agent peut par ailleurs voir engager sa responsabilité civile lorsqu'il commet une faute personnelle. L'établissement, quant-à-lui, pourra généralement voir sa responsabilité engagée en cas de faute ou infraction commise par un employé dont il résulte un dommage, ou lorsqu'un dommage causé dans le cadre des activités de l'établissement résulte du fait ou de l'infraction d'un tiers.

Autrement dit, outre les obligations spécifiques de sécurisation du système d'information dont le non-respect entraîne les sanctions prévues par le texte concerné, lorsqu'elles existent, voire la responsabilité contractuelle de l'établissement[66], une faille ou une mauvaise utilisation des accès réseaux consentis par l'établissement peut également engager la responsabilité de ce dernier, de son président ou de son personnel. Le fondement de cette responsabilité, au delà du respect de la loi, est bien souvent la non prise en compte de l'état de l'art, que constituent par exemple en matière de sécurité des systèmes d'information les normes ISO/IEC[67], le RGS et le guide d'élaboration de politiques de sécurité des systèmes d'information de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[68], ou d'autres documents et recommandations tels que le référentiel de l'ANSSI sur l'archivage électronique sécurisé[69], la recommandation n° 901/DISSI/SCSSI du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense[70] voire les recommandations de la CNIL[71].

La nature de la responsabilité encourue peut être disciplinaire, pénale, civile, ou administrative. Rappelons en brièvement le contenu.

La responsabilité disciplinaire

La responsabilité de l'agent fautif peut en premier lieu être de nature disciplinaire. L'article 29 de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires[72] dispose en effet que « *toute faute commise par un fonctionnaire dans l'exercice ou à l'occasion de l'exercice de ses fonctions l'expose à une sanction disciplinaire* », sanction pouvant être cumulée à une

[63]Voir infra notre sous-titre 2.3.

[64]La confiance des tiers peut être difficile à obtenir en l'absence, notamment, de politique de sécurité du système d'information.

[65]L'image de l'établissement et de son personnel peut être entachée par des erreurs de communication (sur les réseaux sociaux, forums, par email...) ou par des infractions commises par des tiers (une compromission de machine peut par ex. conduire l'établissement à héberger des contenus illégaux ou être la source de spam) voire par le personnel (le dépôt de certains contenus sur un poste ou serveur peut avoir pour résultat l'hébergement par l'établissement de contenus illégaux).

[66]Nous avons vu plus haut (voir supra, notre sous-titre 2.1.2 et notre note de bas de page n° 39) que la responsabilité contractuelle d'un établissement public peut être engagée en cas d'inexécution de ses obligations, par exemple en cas de non respect d'une obligation de confidentialité prévue par un accord de collaboration.

[67]Exemple des normes ISO/IEC 27000 et suivantes.

[68]Ce guide est disponible sur le site de l'ANSSI à l'adresse http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/pssi-guide-d-elaboration-de-politiques-de-securite-des-systemes-d-information.html.

[69]Ce référentiel est disponible sur le site de l'ANSSI à l'adresse http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/archivage-electronique-securise.html.

[70]Cette recommandation est disponible sur le site de l'ANSSI à l'adresse http://www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf.

[71]Voir notamment CNIL, 10 conseils pour la sécurité de votre système d'information, article du 12 octobre 2009, http://www.cnil.fr/la-cnil/actu-cnil/article/article/10-conseils-pour-securiser-votre-systeme-dinformation-1/.

[72]Disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=391E54D86D2BA3E0840B8E2086567A28.tpdjo09v_1?cidTexte=JORFTEXT000000504704&dateTexte=20111017.

responsabilité pénale. Dans les universités, les enseignants contractuels et les étudiants peuvent également faire l'objet de mesures disciplinaires[73].

La responsabilité pénale

La responsabilité de l'agent fautif, voire de l'établissement lui-même, peut en deuxième lieu être de nature pénale.

Tout d'abord, un fonctionnaire, un agent non titulaire ou le chef d'établissement peut être l'auteur d'une infraction, lorsqu'il concentre en sa personne l'élément matériel et l'élément moral[74] de cette infraction, telle que le droit pénal la définit. Est considéré comme auteur de l'infraction celui qui commet les faits incriminés, mais encore celui qui tente de commettre un crime, ou, lorsque la loi le prévoit, un délit[75]. Ainsi, par exemple, en sa qualité de responsable d'un traitement de données à caractère personnel[76], le chef d'établissement encourt cinq ans d'emprisonnement et 300 000 euros d'amende s'il procède ou fait procéder à un traitement de données sans mettre en œuvre les mesures de sécurité prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[77]. La Cour de cassation, dans un arrêt du 30 octobre 2001, a d'ailleurs confirmé un arrêt de cour d'appel qui retenait la responsabilité pénale des président et directeur d'un syndicat pour défaut de sécurité d'un traitement de données à caractère personnel, en ce qu'ils n'avaient pas fait assurer de formation suffisante aux utilisateurs du système automatisé afin qu'ils en maîtrisent le fonctionnement, une telle maîtrise étant de nature à empêcher la divulgation de données personnelles à des personnes illégitimes[78]. Pourrait encore être condamné pénalement, sous réserve de son identification, le tiers responsable d'une compromission de machine de l'établissement[79] qui aurait pour effet, par exemple, l'hébergement de contenus illégaux sur les serveurs de l'université, ou l'accès illégitime de ce tiers à des informations confidentielles. En revanche, il convient de noter qu'en l'absence de toute sécurisation, l'auteur d'une intrusion informatique semble ne pas pouvoir être poursuivi, selon un arrêt de la Cour d'appel de Paris en date du 30 octobre 2002[80].

Ensuite, un fonctionnaire, un agent non titulaire ou le chef d'établissement peut être considéré comme étant le complice d'une infraction, et sera puni en conséquence comme s'il en était l'auteur[81], même si l'auteur réel n'est pas condamné voire connu[82], s'il en facilite sciemment la préparation ou la commission par aide ou assistance, ou si par don, promesse, menace, ordre, abus d'autorité ou de pouvoir il provoque à une infraction ou donne des instructions pour la commettre (ce dernier cas étant le seul permettant de réprimer la complicité en matière de contraventions, sauf disposition spécifique contraire)[83]. L'acte de complicité est en principe un acte positif, mais la jurisprudence a pu admettre des cas de complicité passive, lorsque la personne en cause s'est abstenue d'intervenir alors que sa fonction était précisément d'agir[84]. L'acte de complicité doit encore être intentionnel et intervenir avant ou de manière concomitante à l'infraction, ce qui signifie que la complicité ne peut généralement plus être constatée après la réalisation de l'infraction, sauf si cette infraction est qualifiée de « continue », c'est-à-dire si la définition de cette infraction dans la loi inclut une

---

[73]Voir notamment L'article 712-4 du code de l'éducation, l'article 40 du décret n° 92-657 du 13 juillet 1992 relatif à la procédure disciplinaire dans les établissements publics d'enseignement supérieur placés sous la tutelle du ministre chargé de l'enseignement supérieur (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006079467&dateTexte=vig), ainsi qu'une chronique sur le contentieux disciplinaire sur le site Jurisconsulte.net du cabinet d'avocats André Icard : http://www.jurisconsulte.net/fr/chroniques-video/theme-184-contentieux-disciplinaire/id-534-quid-de-la-procedure-disciplinaire-en-cas-de-fraude-aux-examens-.

[74]L'élément moral de l'infraction est différent selon les textes. Il correspond généralement à une « intention » de commettre l'acte matériel puni par la loi pénale. Il s'agit au minimum d'une « conscience » de violer la loi, autrement dit d'accomplir un acte que l'on sait interdit. Certains textes exigent toutefois, en plus de cette conscience, une volonté spéciale, qui est la conscience de provoquer un préjudice, ou la recherche d'un résultat que l'on sait défendu. Enfin, d'autres textes ne requièrent qu'une faute d'imprudence ou de négligence, sorte de volonté « affaiblie » *:* voir l'art. 121-3 al. 3 du code pénal, et par ex. son art. 226-16, sachant que cet article L. 121-3 s'applique de manière un peu différente en ce qui concerne les fonctionnaires (voir l'article 11 bis 1 de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires). Le 4ème alinéa de l'article 121-3 du c. pénal, prévoit enfin la responsabilité pénale des personnes physiques qui n'ont contribué qu'indirectement au dommage, sous certaines conditions. Cette dernière forme de responsabilité ne concerne pas, a priori, les obligations et enjeux juridiques abordés dans la présente étude. Pour approfondir cette question de l'élément moral voir par ex. E. De Marco, *L'anonymat sur Internet et le droit*, op. cit. en note 7.

[75]Article 121-4 du code pénal.

[76]Le responsable d'un traitement de données à caractère personnel est, selon l'article 3 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *« la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* », « *sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement* ».

[77]Voir supra, notre sous-titre 2.1.2.1.

[78]Cass. crim., 30 octobre 2001, n° de pourvoi 99-82136, non publié au bulletin, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007604461&fastReqId=217151445&fastPos=1, http://lexinter.net/JPTXT2/negligence_et_acces_a_des_donnees_protegees.htm.

[79]Par exemple (et notamment) sur le fondement de l'article 323-1 du code pénal, qui réprime le fait « *d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un* système *de traitement automatisé de données* ».

[80]CA Paris, 30 octobre 2002, Antoine C. vs Ministère public, société Tati, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=136 : Les *« parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, qui ne font, par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, (doivent) être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ».*

[81]Article 121-6 du code pénal.

[82]Voir par ex. Jacques-Henri Robert, Droit pénal général, 4ème éd., mai 1999, coll. Themis droit privé, PUF, p. 345.

[83]Article 121-7 du code pénal. Voir également par ex. Jacques-Henri Robert, Droit pénal général, op. cit., p. 333, 342.

[84]Jacques-Henri Robert, précité, p. 335.

condition de persistance[85]. Ainsi, le recel[86], qui est notamment le fait de bénéficier intentionnellement du produit d'un crime ou d'un délit, ou de détenir une chose en sachant qu'elle provient d'un crime ou d'un délit, est une infraction continue. Dès lors, dans l'hypothèse où les juges considéreraient que le responsable informatique a pour fonction d'agir dans ce type de situations (la complicité par inaction restant exceptionnelle), il est possible d'imaginer que ce dernier, informé et inactif, puisse être qualifié de complice de recel, si un membre du personnel utilisait en connaissance de cause un logiciel contrefait, ou si une machine de l'établissement hébergeait une contrefaçon (sous réserve également, dans cette dernière hypothèse, qu'un tel hébergement soit considéré comme l'un des éléments constitutifs d'un recel, lui-même en cours lors de la prise de connaissance suivie d'inaction du responsable informatique[87]).

Enfin, la responsabilité de la personne morale elle-même peut-être engagée, lorsque l'infraction est commise par l'un de ses organes ou représentants, pour le compte de cette personne morale. Ces notions d' « organes » ou de « représentants » peuvent être interprétées assez largement par les juges, qui n'excluent notamment pas les faits commis par des personnes pourvues « *de la compétence, de l'autorité et des moyens nécessaires, ayant reçu délégation de pouvoirs de la part des organes de la personne morale ou une subdélégation des pouvoirs d'une personne ainsi déléguée* »[88]. Si la délégation administrative ne répond pas exactement aux critères de la délégation de pouvoirs en droit privé[89], il ne reste pas exclu que « *de simples agents* », autres que le président de l'établissement ou les instance habilitées à décider pour cet établissement puissent engager la responsabilité de ce dernier[90]. Une personne morale peut enfin être déclarée responsable même si son organe ou représentant n'a pas été déclaré personnellement responsable des faits constitutifs de l'infraction[91] voire n'a pas été identifié[92]. Inversement, la responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits[93].

La responsabilité civile

En cas de faute personnelle, la responsabilité de tout agent public peut être recherchée devant les juridictions de l'ordre judiciaire sur le fondement des articles 1382 et 1383 du code civil, dès lors que la victime démontre une faute ou une négligence à l'origine d'un dommage, et le lien de causalité qui les unit[94].

Une faute personnelle est une faute qui est commise en dehors du service et sans lien avec ce dernier (par exemple, constituerait sans doute une faute personnelle une diffamation effectuée sur un forum à l'aide d'un terminal personnel hors du temps de travail), par opposition à la faute dite « de service », qui est une faute commise par un agent dans l'exercice de ses fonctions et qui est « impersonnelle », c'est-à-dire qui aurait pu être commise par un autre agent dans les mêmes conditions, et qui entraîne non la responsabilité de l'agent mais celle de l'administration, devant les juridictions administratives[95]. Il existe ceci dit des fautes personnelles qualifiées de « n*on détachables du service* », ou « *non dépourvues de tout lien avec le service* », qui sont des fautes personnelles commises soit « *à l'occasion du service* », soit avec des moyens fournis par le service, voire des fautes commises dans « *l'exercice même des fonctions* », mais qui ne peuvent être considérées comme de simples fautes de service, par exemple en raison de leur gravité[96]. En cas de faute personnelle non détachable du service, qui correspond en définitive à la juxtaposition d'une

[85]Jacques-Henri Robert, précité, p. 206.

[86]Article 321-1 du code pénal.

[87]Une personne devrait détenir la contrefaçon ou en bénéficier en sachant qu'il s'agit d'une contrefaçon, au moment de la prise de connaissance suivie d'inaction du responsable informatique. Notons par ailleurs que les juges ont déjà pu considérer que le téléchargement d'une œuvre sur des réseaux peer-to-peer n'était pas un acte de recel (voir Jean-Louis Fandiari, « A Bayonne, les téléchargeurs ne sont pas des receleurs », 16 mai 2005, juriscom.net, http://www.juriscom.net/actu/visu.php?ID=764). Une polémique persiste également sur le fait de savoir si le téléchargement d'une œuvre à partir d'une matrice illégale est une copie privée ou un acte de contrefaçon (voir Estelle De Marco, « *Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux* », 4 juin 2009, Juriscom.net, http://www.juriscom.net/uni/visu.php?ID=1133, p. 6). Dans la première hypothèse, il ne pourrait a priori y avoir recel, car la chose proviendrait d'un acte permis par la loi.

[88]Cass. crim., 26 juin 2001, n° de pourvoi 00-83.466, disponible sur Legifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007067413&fastReqId=1459264686&fastPos=1. Sur la notion de représentant, voir également Emmanuelle Lemoine, *La répression de l'indifférence sociale en droit pénal français*, L'Harmattan, 2002, n° 166, n° 182 et s.

[89]Voir par exemple Fabrice Belghoul, « L'extension de la responsabilité pénale des personnes morales », mémoire de DEA, disponible sur le site du village de la justice, http://www.village-justice.com/journal/articles/ftp/responsabilitepenale.pdf, p. 20 et s.

[90]Voir par exemple « La responsabilité civile, pénale et administrative en matière d'hygiène et de sécurité », Centre national de la recherche scientifique et technique (CNRS), pp. 12 et 13, disponible sur le site du CNRS à l'adresse http://www.dr1.cnrs.fr/docs_pdf/ps/supports/responsabilite.pdf .

[91]« La responsabilité civile, pénale et administrative en matière d'hygiène et de sécurité », op. cit., p. 12, citant une décision de la Cour de cassation du 12/12/2000.

[92]Voir par ex. Emmanuelle Lemoine, *La répression de l'indifférence sociale en droit pénal français*, op. cit., n° 169.

[93]Article 121-2 du code pénal.

[94]Pour de plus amples développements relatifs à la responsabilité délictuelle, voir par ex. Amandine Assaillit, « Les fondements de la responsabilité civile délictuelle », oct. 2006, http://www.masterdroit.fr/3_Ressources_Fiches_fichiers/FICHES_PDF/FICHES_RESP_PDF/1_Les_fondements_responsabilite_civile_delictuelle.pdf.

[95]Michel Paillet, « Existe-t-il une responsabilité de droit commun ? », n°20, in *Actes du colloque : vers de nouvelles normes en droit de la responsabilité publique*, Palais du Luxembourg, 11 et 12 mai 2001, http://www.senat.fr/colloques/colloque_responsabilite_publique/colloque_responsabilite_publique_mono.html), Maryse Geguergue, « Y a t-il une "subsidiarisation" dans le droit de la responsabilité administrative ? », II, A, in *Actes du colloque : vers de nouvelles normes en droit de la responsabilité publique,* op. cit.) ; le lexique juridique de Shirley Leturcq, Avocat, http://www.avocat-droit-public-marseille.fr/fr/lexique-juridique/id-144-faute-de-service.

[96]Voir par ex. Monique Tranquard, « Responsabilité des membres de l'enseignement public et TIC », Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche – SDTICE, mars 2006, disponible à partir des adresses http://www.infotheque.info/ressource/9469.html et http://eduscol.education.fr/legamedia/guide/responsabilite-enseignant, et à l'adresse http://eduscol.education.fr/chrgt/responsabilite-enseignant.pdf, p. 12.

faute personnelle et d'une faute de service, donc d'une faute de l'agent et d'une faute de l'administration, les victimes ont la possibilité d'agir à leur choix devant les juridictions de l'ordre judiciaire ou devant les juridictions administratives, l'administration disposant ensuite d'une « action récursoire » contre son agent devant les tribunaux administratifs, afin de demander à cet agent le remboursement des dommages et intérêts qu'elle a versés à la victime[97].

Par ailleurs, la responsabilité des membres de l'enseignement public peut être engagée soit à raison des dommages causés par « *les élèves ou les étudiants qui leur sont confiés à raison de leurs fonctions* », soit à raison des dommages causés au détriment de ces élèves ou étudiants[98]. Il en est notamment ainsi « *toutes les fois que, pendant la scolarité ou en dehors de la scolarité, dans un but d'enseignement ou d'éducation physique, non interdit par les règlements, les élèves et les étudiants confiés (...) aux membres de l'enseignement public se trouvent sous la surveillance de ces derniers* »[99]. Si cette notion de surveillance exclut en principe l'enseignement supérieur du champ d'application de la loi, puisque « *les enseignants n'y ont pas la "garde" des étudiants* »[100], « *le concept de surveillance peut cependant ressurgir lors de certaines activités spécifiques, notamment pour les activités sportives dirigées par un enseignant dans le cadre du cursus universitaire* »[101]. Il est ainsi possible d'imaginer qu'il puisse recevoir application dans le cadre de certaines activités liées à l'utilisation des réseaux informatiques. En cas d'engagement de la responsabilité des membres de l'enseignement public pour défaut de surveillance[102], l'action doit être dirigée contre l'État et non contre l'enseignant concerné, devant les juridictions de l'ordre judiciaire. L'État dispose par contre d'une action récursoire contre le membre de l'enseignement public concerné ou contre les tiers[103], afin d'obtenir le remboursement des sommes qu'il a versées à la victime.

La responsabilité administrative

Lorsque la faute d'un agent public ou d'un agent non titulaire peut être qualifiée de faute de service, la victime doit engager la responsabilité de l'administration devant le juge administratif et démontrer la faute, un préjudice direct, certain et spécial, matériel ou moral, et un lien de causalité entre les deux[104]. En cas de faute personnelle non détachable du service, comme nous l'avons vu, la victime peut d'ailleurs également saisir la juridiction administrative, au lieu du juge civil, l'administration disposant dans ce dernier cas d'une action récursoire contre son agent. Une sécurisation insuffisante du système d'information ayant pour résultat une compromission, entraînant elle-même un dommage (exposition d'un tiers à des contenus illégaux, accès à des données personnelles, destruction de résultats d'examen, dommage causé à l'ordinateur d'un visiteur voire, au-delà du champ de notre étude, à un internaute ayant consulté le site web de l'établissement...), pourrait ainsi sans aucun doute conduire à une demande d'indemnisation devant le juge administratif, sur la base d'une faute de service (du RSSI, sans doute, dans la plupart des cas), voire d'une faute personnelle non détachable du service (auquel cas l'administration disposerait d'une action récursoire contre l'agent fautif). La responsabilité de l'établissement pourrait encore être recherchée dans le cas où un employé publierait un site personnel contrefaisant et injurieux grâce aux moyens fournis par l'établissement. En effet, le TGI de Marseille et la Cour d'Aix-en-Provence, dans une affaire Escota vs Lucent et autres[105], ont considéré que l'employeur était dans une telle situation responsable des agissements de son salarié sur la base des dispositions de l'article 1384 du code civil, lequel prévoit la responsabilité du commettant pour les faits de son préposé lorsque certaines causes d'exonération ne sont pas réunies[106], causes dont l'absence de réunion caractérise également la faute de service (une faute personnelle complémentaire n'étant ceci dit pas exclue).

La responsabilité de l'administration peut encore être engagée en cas de défaut d'organisation du service public de l'enseignement. Cette notion n'est pas définie par les textes, mais selon un auteur, elle peut notamment « *résulter d'une inertie ou d'une carence dans l'organisation de l'établissement, voire d'erreurs dans l'appréciation des moyens à mettre en œuvre par le service pour assurer sa mission* »[107]. Elle peut encore parfois être engagée sans faute, un exemple applicable à l'usage des technologies de l'information

---

[97] « La responsabilité civile, pénale et administrative en matière d'hygiène et de sécurité », précité, p. 7.

[98] Formules de l'article L. 911-4 du code de l'éducation.

[99] Article L. 911-4 al. 2 du code de l'éducation.

[100] Monique Tranquard, op. cit., p. 16.

[101] Monique Tranquard, op. cit., p. 16, faisant référence à une décision du Tribunal des conflits en date du 20 décembre 1985.

[102] Sur les conditions d'engagement de la responsabilité des enseignants, voir Monique Tranquard, op. cit., notamment pp. 18-22.

[103] Article L. 911-4 du code de l'éducation.

[104] Pour de plus amples développements sur ces notions, voir Monique Tranquard, op. cit., pp. 5-9.

[105] TGI Marseille, 11/06/03, http://www.legalis.net/breves-article.php3?id_article=234 ; CA Aix-en-Provence, 13/03/06 http://www.juriscom.net/jpt/visu.php?ID=807.

[106] L'employeur ne peut s'exonérer que lorsque le préposé, « *agissant sans autorisation, à des fins étrangères à ses attributions, s'est placé hors des fonctions auxquelles il était employé* » (voir par ex. Dominique Broggio, *L'évolution de la responsabilité du chef d'entreprise*, mémoire de DEA, Université René Descartes – Paris 5, http://www.droit.univ-paris5.fr/AOCIVCOM/01memoir/BroggioM.pdf, p. 13, citant notamment un arrêt de l'assemblée plénière en date du 17 juin 1983). Dans l'affaire Escota vs Lucent, les juridictions ont estimé qu'un technicien test utilisant Internet quotidiennement avait agi « *dans le cadre de ses fonctions* » ; que le droit dont il disposait de consulter d'autres sites sans interdiction spécifique concernant la réalisation de sites internet ou la publication sur des pages personnelles équivalait à une « *autorisation* » de l'employeur ; que le droit dont il disposait d'accéder à Internet y compris hors de ses heures de travail impliquait que son méfait n'avait pas de « *fins étrangères à ses attributions* ». Pourtant, l'employeur avait adressé une note à ses salariés, les autorisant à utiliser les accès réseaux « *pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité* », tout en précisant que ces utilisations devaient être raisonnables, devaient s'effectuer en dehors des heures de travail, devaient respecter les dispositions légales et les règles internes de l'entreprise en cause, les sites à caractère explicitement sexuel et contrevenant aux valeurs de cette entreprise étant expressément prohibés.

[107] Monique Tranquard, op. cit., p. 28.

et de la communication (TIC) dans les établissements publics étant la responsabilité sans faute au titre de la rupture devant les charges publiques, dans l'hypothèse où « *certains usages des TIC (pourraient) causer des préjudices spéciaux* » à des étudiants[108].

2.3 Les droits et obligations des établissements dans le cadre de la démarche de sécurisation

Les obligations de sécurisation comme le droit de sécuriser impliquent le droit de prendre certaines mesures en vue de la sécurisation du système d'information et de son utilisation, ce droit connaissant lui-même certaines limites. Sans prétendre à l'exhaustivité, nous ne traiterons ici que de mesures nous paraissant particulièrement importantes à aborder, compte tenu notamment de leur sensibilité particulière ou de leur caractère parfois méconnu[109]. Il s'agit des activités de surveillance, journalisation et analyse ; de l'information, formation et implication des utilisateurs ; de la mise en place de chartes ; de la question du filtrage et de la conduite à tenir en cas d'infraction.

Surveillance, journalisation, analyse...

Les opérateurs ont l'interdiction de surveiller les activités de leurs abonnés, notamment aux termes de l'article L. 34-1 du CPCE, qui pose un principe d'effacement ou d'anonymisation des données de trafic. Il semble judicieux de transposer cette règle aux établissements publics d'enseignement supérieur s'agissant des activités en ligne de leurs étudiants et visiteurs, puisque les dispositions de l'article L. 34-1 leur sont applicables, en leur qualité de FAI « à titre accessoire »[110], en plus généralement en raison de l'importance accordée à la protection de la vie privée.

Ceci dit, le principe étant posé, les opérateurs et les établissements publics d'enseignement supérieur ont la possibilité de « *conserver certaines données en vue d'assurer la sécurité de leur réseau* », aux termes de l'article L. 34-1, III du CPCE. Ces données, précisées par le décret n°2006-358 du 24 mars 2006[111], sont les données techniques permettant d'identifier le ou les destinataires de la communication, les données permettant d'en identifier l'origine, les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication, et les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs. Les données conservées ne doivent en revanche porter que *« sur l'identification des personnes* » qui utilisent leurs services, sur « *les caractéristiques techniques des communications assurées* » et sur « *la localisation des équipements terminaux ».* Ces données ne peuvent en revanche « *en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelques forme que ce soit, dans le cadre de ces communication*s »[112]. L'ensemble de ces traitements sont par ailleurs soumis au respect des dispositions de la loi du 6 janvier 1978[113].

Dans l'entreprise, inversement, l'employeur a selon les juges « *le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail* »[114], décision a priori transposable aux établissements publics d'enseignement supérieur s'agissant de leurs employés. Toutefois, ce contrôle reste soumis aux principes de finalité, de transparence et de proportionnalité, qui transparaissent tant des dispositions de la loi du 6 janvier 1978[115] que des principes dégagés par la Cour européenne des droits de l'Homme[116].

---

[108]Monique Tranquard, op. cit., p. 10.

[109] Nous ne traiterons notamment pas du chiffrement (art. 30 de la loi n° 2004-575 pour la confiance dans l'économie numérique) ou de la signature électronique (1316-4 du code civil et décret n° 2001-272 du 30 mars 2001, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796).

[110]Voir supra, notre titre 1.

[111]Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, JORF n° 73 du 26 mars 2006 page 4609, texte n°9, disponible sur Légifrance à l'adresse http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=892A512993CBD3E6B530AD56F27BC215.tpdjo09v_1?cidTexte=JORFTEXT000000637071&dateTexte=20111017.

[112]Art. L. 34-1, VI du code des postes et des communications électroniques.

[113]Art. L. 34-1, VI du code des postes et des communications électroniques.

[114]Voir par exemple Cass. soc. 7 juin 2006, pourvoi n° 04-43866, disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007053295&fastReqId=2091098120&fastPos=4.

[115]Ces dispositions imposent que « *tout traitement de données personnelles soit déclaré à la CNIL, que les (employés) soient informés de son existence, de ses finalités, de ses caractéristiques et qu'ils aient accès aux données les concernant* » : Hubert Bouchet, *La cybersurveillance sur les lieux de travail,* rapport adopté par la CNIL le 5 février 2002, La documentation française, mars 2004, http://www.ladocumentationfrancaise.fr/rapports-publics/044000175/index.shtml et (adresse directe) http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf, p. 6.

[116]Voir par exemple le document de travail concernant la surveillance des communications électroniques sur le lieu de travail du groupe de travail « article 29 » sur la protection des données, 29 mai 2002, WP 55, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_fr.pdf. Le groupe de travail préconise, à la lumière tant de la directive 95/46/CE que de la *« jurisprudence de la Cour européenne des droits de l'Homme concernant l'article 8 »* de la convention éponyme et *« d'autres textes internationaux pertinents* », que toute mesure de surveillance soit évaluée à la lumière de plusieurs critères avant d'être mise en œuvre sur le lieu de travail, ces critères étant la transparence, la nécessité, la proportionnalité de la mesure à son objectif et le caractère équitable du traitement de données personnelles pour les employés (voir p. 4 du document de travail). Voir également, par exemple, l'arrêt de la Cour de cassation, chambre sociale, en date du 9 juillet 2008, Franck L. vs entreprise Martin, disponible sur le site web de legalis.net : « *qu'il résulte de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, de l'article 9 du code civil, de l'article 9 du code de procédure civile et de l'article L. 120-2* [ancien art. 1121-1, ndla] *du code du travail que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret de ses communications* ».

En conséquence, la mesure de contrôle devra notamment faire l'objet d'une consultation des instances représentatives du personnel[117], d'une information des salariés[118] et d'une déclaration ou d'une demande d'autorisation auprès de la CNIL[119].

Cette mesure devra encore veiller à ne pas limiter la vie privée de l'employé de manière disproportionnée. Ainsi, la Cour de cassation considère que les connexions établies sur des sites Internet pendant le temps de travail[120] et les dossiers et fichiers créés par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur[121], sont présumés avoir un caractère professionnel, l'employeur pouvant dès lors les consulter hors la présence du salarié, sauf lorsque les dossiers et fichiers en cause sont identifiés comme étant personnels[122]. L'employé devra inversement être présent ou dûment appelé lors de la consultation de dossiers et de fichiers personnels[123], de même que pour l'inspection du disque dur en vue de vérifier les connexions Internet effectuées en dehors du temps de travail, sauf, dans l'une et l'autre de ces hypothèses, « *risque ou événement particulier* »[124]. En revanche, l'employeur ne peut jamais ouvrir les correspondances personnelles de ses employés, qu'il s'agisse de courriers postaux[125] ou de « *messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* »[126]. Il appartient dès lors à l'employé d'identifier clairement ses messages personnels comme étant tels, les modalités de cette identification pouvant être prévues dans une charte d'utilisation des moyens informatiques[127].

Que l'établissement public d'enseignement supérieur agisse en qualité d'opérateur ou d'employeur, il reste encore à noter que ses administrateurs réseaux se voient reconnaître le droit de prendre connaissance des contenus personnels des utilisateurs, incluant le contenu des messageries, dans un objectif de sécurité, sous réserve d'en préserver la confidentialité[128].

---

[117]Il s'agit dans les universités du comité technique, prévu par l'article L 951-1-1 du code de l'éducation, qui doit notamment être consulté « *sur les questions et projets de textes relatifs (…) aux évolutions technologiques et de méthode de travail des administrations, établissements ou services et à leur incidence sur les personnels* » (décret n° 2011-184 du 15 février 2011 relatif aux comités techniques dans les administrations et les établissements publics de l'État, http://legifrance.gouv.fr/affichTexte.do;jsessionid=2CE6C4160F8474E1DD4C486350FF15DE.tpdjo09v_1?cidTexte=JORFTEXT000023592572&dateTexte=20111018. Ce décret se substitue au décret n°82-452 du 28 mai 1982 relatif aux comités techniques paritaires, qui ne demeure applicable qu'à titre transitoire).

[118]La CNIL préconise de les informer *« individuellement, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées ou sauve*gardées ». Elle considère qu'une « durée de conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'Internet ». Elle précise qu'« *en cas d'archivage automatique des messages électroniques, les salariés doivent (...) être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès* ». « *Si des procédures disciplinaires sont susceptibles d'être engagées sur la base de ces fichiers* », ils doivent encore en être « *explicitement informés* » : CNIL, guide pour les employeurs et les salariés, édition 2010, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf, p. 18.

[119]Par exemple, une déclaration « normale » est nécessaire, sauf si un correspondant informatique et liberté a été désigné, lorsque *« l'administration met en place un dispositif de contrôle individuel des (employés) destiné à produire un relevé des connexions ou des sites visités, poste par poste* ». Lorsque « *l'administration met en place un dispositif qui ne permet pas de contrôler individuellement l'activité des salariés, ce dispositif peut faire l'objet d'une déclaration de conformité en référence à la norme simplifiée n° 46 (gestion des personnels des organismes publics et privés)* » : p.19. Inversement, une autorisation de la CNIL sera nécessaire par principe en cas d'utilisation de dispositifs biométriques, sauf si le dispositif projeté est conforme à l'un des cadres déterminés par la CNIL, appelé « autorisation unique » : CNIL, guide pour les employeurs et les salariés, p 35 ; voir également le site de la CNIL, fiche pratique sur la biométrie du 7 avril 2011, http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/biometrie-des-dispositifs-sensibles-soumis-a-autorisation-de-la-cnil/.

[120]Cass soc. 9 juillet 2008, Franck L. v. Entreprise Martin, n° de pourvoi 06-45800, disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000019166094&fastReqId=398466071&fastPos=4.

[121]Cass. soc. 18 octobre 2006, n° de pourvoi 04-48025, disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007054915&fastReqId=1174707376&fastPos=4 ; Cass. soc. 21 octobre 2009, n° de pourvoi 07-43877, disponible à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000021194925&fastReqId=1759598261&fastPos=5 ; Cass. soc. 15 décembre 2009, n° de pourvoi 07-44264, disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000021512309&fastReqId=477518922&fastPos=19.

[122] Cass. Soc. 18/10/2006, 21/10/2009 et 15/12/2009 précités. Ne sont pas considérés comme étant identifiés comme personnels les fichiers intitulés « essais divers, essais divers B, essais divers restaurés » (Cass. Soc. 15/12/2009, précité), ou les fichiers d'un sous-répertoire nommé « Marteau », présents dans un répertoire nommé « personnel », lui-même placé dans un répertoire nommé « JM », ces deux lettres correspondant aux initiales de l'employé (Cass. Soc. 21/10/09, précité).

[123]Cass. soc. 15 décembre 2009, précité.

[124]Cass. soc. 9 juillet 2008, précité.

[125]S'agissant des connexions Internet voir Cass, ch. mixte, 18 mai 2007, n° de pourvoi 05-40803, disponible sur le site de Légifrance à l'adresse *http://www.legifrance*.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000017849284&fastReqId=379603697&fastPos=2. S'agissant des dossiers et fichiers personnels, voir Cass. Soc. 17 mai 2005, n° de pourvoi 03-40017, disponible sur le site de Légifrance à l'adresse http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007048803&fastReqId=696357997&fastPos=2. Dans cette dernière décision, la Cour de cassation considère que ne constitue pas un risque ou événement particulier le contrôle effectué à l'occasion de la découverte de photos érotiques n'ayant aucun lien avec l'activité de l'employé, quand bien même l'accès au disque dur « *était libre, aucun code personnel n'ayant été attribué au salarié pour empêcher toute autre personne que son utilisateur d'ouvrir les fichiers* ».

[126]Cass. soc., 2 octobre 2001, arrêt dit « Nikon », n° de pourvoi 99-42942, disponible sur le site de Légifrance à l'adresse *http://www.legifrance*.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007046161&fastReqId=453088670&fastPos=20.

[127]Voir infra, « Chartes ».

[128]CA Paris, 11ème chambre, 17 décembre 2001, disponible sur le site de Legalis.net à l'adresse http://www.legalis.net/?page=jurisprudence-decision&id_article=1182 : « *Il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne, entre autre, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles. (…)*». « *La préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait - de la même façon que la poste doit réagir à un colis ou une lettre suspecte. Par contre, la divulgation du contenu des messages (…) ne relevait pas de ces objectifs* ».

Information, formation, implication...

Au delà de l'obligation d'information des employés sur les mesures de surveillance qui peuvent leur être appliquées, il paraît nécessaire de sensibiliser le personnel et les étudiants aux risques et responsabilités pouvant être générés par l'utilisation des accès réseaux, de les former aux règles de bases de la sécurité informatique, et, dans la mesure du possible, de les impliquer dans la définition de règles communes, pour favoriser la compréhension de ces règles, leur bon accueil et leur respect.

Chartes

La formalisation des règles d'utilisation des ressources informatiques au sein d'une charte du même nom ou « charte de comportement »[129] est également vivement recommandée, comme prolongement naturel de la politique de sécurité du système d'information[130]. De telles chartes, reconnues par la jurisprudence[131], précisent idéalement les droits et devoirs de leurs différents destinataires que peuvent être notamment les administrateurs réseaux, le personnel, les étudiants ou les visiteurs. En termes de contenu[132], elles doivent s'efforcer d'être complètes et à jour, en abordant l'ensemble des équipements et applications mis à la disposition de leurs destinataires, et en précisant les sanctions encourues en cas de comportement fautif. Les chartes peuvent par exemple être l'occasion de définir la manière d'identifier le caractère « privé » des dossiers et messages électroniques du personnel, ou de définir « *les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent* »[133]. Enfin, pour être opposables aux employés, étudiants et visiteurs, la charte doit être annexée au règlement intérieur, ou alternativement signée par chacun d'entre eux.

Filtrage ?

Les FAI ont une obligation de neutralité au regard du contenu des messages transmis sur leur réseau[134], ce qui implique qu'ils ne peuvent mettre en place de mesures de filtrage qui ne seraient pas nécessaires à la sécurité du réseau, à l'intégrité et à la continuité du service[135], ou qui ne seraient pas librement acceptées par l'utilisateur. Ceci, d'autant plus que la liberté d'accès à Internet est protégée par le Conseil constitutionnel sous le visa du droit à la liberté d'expression[136].

Ceci étant dit, les établissements publics d'enseignement supérieur n'ont pas pour objet de mettre un accès Internet à disposition du public, mais, en premier lieu, de participer au service public de l'éducation. En ce sens, il n'est pas inconcevable d'admettre que ces établissements puissent mettre en place, s'ils le souhaitent, des dispositifs de filtrage des ressources qui se révèlent incompatibles ou sans lien avec leurs missions, en leur qualité de titulaire d'un abonnement internet, outre les mesures qu'ils sont légitimes à mettre en œuvre pour assurer leur protection juridique en cette même qualité[137] ou en leur qualité d'établissement public employeur, et celles qui s'avèrent nécessaires à la sécurité du réseau[138]. Ces mesures de filtrage doivent toutefois être réfléchies, afin notamment qu'elles ne constituent pas une entrave au bon fonctionnement de certains services ou activités, voire aux attentes légitimes des étudiants, employés et visiteurs dans ce cadre[139], et qu'elles ne deviennent pas en conséquence une nouvelle source potentielle de responsabilité.

---

[129]Voir par exemple Guillaume Lussier, cours, certificat informatique et internet (C2i), Référentiel A2 « Intégrer la dimension éthique et le respect de la déontologie », Université de Toulouse Le Mirail, 2004, http://didel.script.univ-paris-diderot.fr/claroline/backends/download.php?url=L1EuQy5NLi9DMmlfQTIucGRm&cidReset=true&cidReq=55UTL1107e2.

[130]Dans le même sens, voir CNRS/FSD/Sécurité des Systèmes d'Information, Guide d'élaboration d'une PSSI opérationnelle d'unité, version 1.0 du 23 mai 2008, référence 08.2378/FSD, http://www.dgdr.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/Guide-elaboration-PSSI-operationnelle-unite.pdf, p. 6, principe 4 : « *La Charte utilisateur qui énonce la "loi commune" régissant l'utilisation des moyens informatiques, est le prolongement réglementaire et juridique de la PSSI d'unité* ».

[131]Un « *manquement délibéré et répété du salarié à l'interdiction posée par la charte informatique mise en place dans l'entreprise et intégrée au règlement intérieur* », par des agissements « *susceptibles pour certains de revêtir une qualification pénale* », a été considéré comme constituant une faute grave justifiant le licenciement. : Cass. soc., 15/12/2010, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000023256933&fastReqId=710869507&fastPos=1.

[132]Voir notamment Mascré Heguy Associés, « Charte informatique : comment mettre en place une charte informatique dans l'entreprise ? », fiche point de vue, septembre 2009, http://www.mascre-heguy.com/htm/fr/conseils/conseil_charte_informatique.html.

[133]Voir notamment CNIL, guide pour les employeurs et les salariés, op. cit., pp. 20 et 21.

[134]Articles L..32-1, L.33-1 et D.98-5 du code des postes et des communications électroniques.

[135]Ces exigences constituant également des obligations pour les opérateurs, voir supra notre sous-titre 2.1.1.2.

[136]Conseil constitutionnel, décision 2009-580 DC du 10 juin 2009, JO du 13 juin 2009, p. 9675, http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html, considérant 12 : « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, (le droit à la libre expression) implique la liberté d'accéder à ces services* ».

[137]Voir supra, notamment notre sous-titre 2.1.2.2.

[138]Voir supra, notre sous-titre 2.1.1.2.

[139]Voir par exemple Lionel Dujol, « Le crapaud fou vs Proxynator. Pas facile d'être un bibliothécaire hybride ! », 17 juin 2009, http://labibapprivoisee.wordpress.com/2009/06/17/le-crapaud-fou-vs-proxynator-pas-facile-detre-un-bibliothecaire-hybride/. L'auteur y explique le problème de bibliothécaires souhaitant diffuser les contenus de leur bibliothèque « *sur le web en profitant de l'effet réseau des (…) services 2.0* », dont les réseaux sociaux My Space et Facebook ou des blogs, et qui se heurtent notamment au filtrage de ces services. Ces bibliothécaires ne peuvent dès lors pas plus accompagner l'étudiant dans ses demandes de renseignements relatives à ces services. Voir également Lionel Maurel, « Accès Internet en bibliothèque : ce qu'exige vraiment la loi », http://scinfolex.wordpress.com/2010/03/26/acces-internet-en-bibliotheque-ce-quexige-vraiment-la-loi/, évoquant l'équilibre qui doit être trouvé entre la liberté de l'usager et la responsabilité des bibliothèques, et reprenant la mise au point de l'Interassociation archives bibliothèques documentation (IABD) sur cette question.

En cas d'infraction...

Face à une infraction, il est en premier lieu conseillé à l'organisme concerné d'en préserver les preuves, dans la mesure du possible et sous les réserves vues plus haut tenant à la protection de la vie privée, notamment s'agissant des logs et des preuves présentes sur le disque dur ou un service Internet, par exemple en ayant recours à un huissier spécialisé.

Le signalement de l'infraction peut par ailleurs présenter un intérêt, afin d'éviter tout soupçon de complicité dans la réalisation de cette dernière[140]. Le signalement est en outre dans certaines hypothèses obligatoire. Ainsi, l'article 40 alinéa 2 du code de procédure pénale dispose que « *toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* »[141]. De même, l'article 434-1 du code pénal punit de trois ans d'emprisonnement et de 45000 euros d'amende le fait, « *pour quiconque ayant connaissance d'un crime dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés, de ne pas en informer les autorités judiciaires ou administratives* », les personnes astreintes au secret dans les conditions prévues par l'article 226-13 du code pénal étant exceptées de ces dispositions.

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

Les opérateurs et FAI ont encore à leur charge plusieurs obligations tenant à la lutte contre les infractions et contenus illicites, qui sont ou pourraient être applicables aux établissements publics d'enseignement supérieur. Ces obligations consistent en des obligations de conserver certaines données techniques (3.1), en des obligations de limiter certaines activités réseaux (3.2), et en des obligations d'information et de mise en place de dispositifs de signalement (3.3).

3.1 Obligations de conserver certaines données techniques

Nous avons vu que les opérateurs et les fournisseurs d'accès étaient soumis à une obligation d'anonymisation des données relatives aux utilisateurs de leurs services[142]. Toutefois, ils ont inversement l'obligation, aux termes des dispositions de l'article L. 34-1 du CPCE, de conserver durant un an[143] certaines données relatives au trafic, la non anonymisation comme la non conservation de ces données étant passibles d'un an d'emprisonnement et de 75000 euros d'amende[144]. Les données devant être conservées se trouvent précisées dans le décret n°2006-358 du 24 mars 2006[145] et restent des données techniques, n'imposant pas, a priori, de solliciter et de conserver des éléments relatifs à l'identité de l'utilisateur[146]. Les finalités exclusives de cette conservation sont la mise à disposition, en tant que de besoin, de l'autorité judiciaire, de la haute autorité pour la diffusion des œuvres et la protection des droits sur internet (dite HADOPI)[147], ou, pour certaines de ces données, d' « *agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés* » de la prévention des actes de terrorismes[148]. Les

[140] Voir supra, notre sous-titre 2.2.2, sous « La responsabilité pénale ».

[141]Cette obligation n'est toutefois pas assortie de sanction pénale. Voir par ex. sur ce point André Icard, « Que risque le fonctionnaire qui ne dénonce pas ? », 01/11/2008, http://avocats.fr/space/andre.icard/content/que-risque-le-fonctionnaire-qui-ne-denonce-pas--_2E0B669A-DA87-4931-92F6-009B7EAE6348 ; Gérard Chalon, « Le fonctionnaire et l'article 40 du code de procédure pénale : nature et portée de l'obligation de dénoncer », 01/11/ 2003, revue Actualité juridique. Fonctions publiques (AJFP), nov.-déc. 2003, p. 31.

[142]Voir supra in « Surveillance, journalisation, analyse... ».

[143]À compter de leur enregistrement : article R.10-13, III du CPCE.

[144]Art. L. 39-3 du CPCE. Ces sanctions sont applicables aux opérateurs ou à ceux de leurs agents responsables des faits. Les personnes physiques encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise.

[145]Décret n° 2006-358 du 24/03/06 relatif à la conservation des données des communications électroniques, article 1, créant les articles R10-12 et R10-13 du CPCE. Aux termes de ces articles, les « données relatives au trafic » sont les « *informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi* » (R 10-12). Les données devant être conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales sont les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication 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 (R 10-13). Il convient par contre de noter que l'article R 10-13 indique préciser le contenu de l'obligation prévue au II de l'article L. 34-1 du CPCE, tandis que l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques (précitée) a créé un nouveau II dans ce même article, renumérotant le II en III, sans apparemment modifier le décret en conséquence. Littéralement, ce décret n'est donc plus applicable (la même problématique touche l'article R10-12 mais avec des conséquences moindres, ce dernier renvoyant aux II et au III).

[146]Dans le même sens voir CNIL, « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? », fiche pratique du 28 septembre 2010, http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/conservation-des-donnees-de-trafic/. La conservation des noms, prénoms et adresses des utilisateurs n'étant pas requise par le décret, l'annexe du décret n°2010-236 du 5 mars 2010 relatif au traitement de données autorisé par l'article L. 331-29 du CPI (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021923996&categorieLien=id), qui prévoit que les données recueillies auprès des opérateurs et FAI au titre de l'article L 34-1 du CPCE par la commission de protection des droits de l'HADOPI sont notamment les noms de famille, prénoms et adresse des abonnés, ne trouve par conséquent application que lorsque ces données sont naturellement conservées par le prestataire en cause.

[147]Article L.34-1 du code des postes et des communications électroniques.

[148]Article L. 34-1-1. « *Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* » (alinéa 2).

prestataires de services ont par ailleurs l'obligation, depuis l'ordonnance n° 2011-1012 du 24 août 2011, d'établir dans ce cadre « *des procédures internes permettant de répondre aux demandes des autorités compétentes* »[149]. Ces traitements sont enfin soumis au respect des dispositions de la loi du 6 janvier 1978[150].

Les fournisseurs d'accès à Internet, comme les fournisseurs d'hébergement, ont également l'obligation de conserver « *les 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 elles sont prestataires* », aux termes de l'article 6, II de la loi n°2004-575 du 21 juin 2004[151]. Ces données, précisées par le décret n° 2011-219 du 25 février 2011[152], consistent également en des données techniques, excluant les données d'identité lorsque ces dernières ne sont pas collectées habituellement[153]. L'autorité judiciaire peut en requérir communication, de même que les agents habilités en matière de prévention du terrorisme que nous mentionnions au paragraphe précédent[154]. Ces données doivent là encore être conservées pendant un an[155], dans des conditions permettant « *une extraction dans les meilleurs délais pour répondre à une demande des autorités judiciaires* »[156], et dans le respect des dispositions de la loi du 6 janvier 1978[157]. La non conservation de ces données est sanctionnée d'un an d'emprisonnement et de 75000 euros d'amende[158].

L'application de ces dispositions aux établissements publics d'enseignement supérieur fait peu de doutes, s'agissant de l'accès qu'ils offrent à leurs étudiants et visiteurs, comme nous l'avons vu dans notre première partie. Leur application dans le cadre de l'accès que ces établissements fournissent à leurs employés est moins certaine[159], bien que le risque juridique d'une non conservation puisse être important, compte tenu de la décision de la Cour d'appel de Paris en date du 4 février 2005[160]. Cette application aux employés ne semble ceci dit pas poser de problème particulier[161], tenant la possibilité pour l'employeur de contrôler l'activité de ces derniers dès lors que les garanties appropriées sont mises en place[162].

3.2 Obligations de limiter certaines activités réseaux

Les fournisseurs d'accès à Internet ont à leur charge des obligations de filtrage dans deux hypothèses.

En premier lieu, ils doivent mettre en place les mesures de filtrage que leur impose le juge. Ce dernier peut en effet prescrire aux FAI « *l'arrêt de l'accès* » d'un service de jeux ou paris en ligne non autorisés en vertu d'un droit exclusif ou d'un agrément délivré par l'autorité de régulation des jeux en ligne, sur saisine de cette autorité[163]. Il peut encore ordonner une mesure de filtrage en matière

[149]Article L. 34-1 du code des postes et des communications électroniques, alinéa 3, tel que modifié par l'article 7 de l'ordonnance 2011-1012, précitée.

[150]Art. L. 34-1, VI du code des postes et des communications électroniques.

[151]Loi pour la confiance dans l'économie numérique, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=.

[152]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, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id.

[153] Il s'agit de l'identifiant de la connexion, de l'identifiant attribué par ces personnes à l'abonné ; de l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ; des dates et heure de début et de fin de la connexion ; des caractéristiques de la ligne de l'abonné. Les FAI doivent encore conserver certaines autres données recueillies dans le cadre de la souscription d'un contrat, telles que les nom, prénom et adresses de l'utilisateur, mais ceci uniquement « *dans la mesure où (ils) les collectent habituellement* » (article 1 du décret, dernier alinéa).

[154]Article 6, II bis de la loi n° 2004-575.

[155]Article 3 du décret n°2011-219. Ce délai court à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu (création initiale, modification, suppression), ou, s'agissant des données à ne conserver que lorsqu'elles sont collectées habituellement, à compter de la résiliation du contrat ou de la fermeture du compte, et à compter de la date d'émission de chaque facture ou opération de paiement.

[156]Article 4 du décret n°2011-219.

[157]Article 4 du décret n°2011-219 et art. 6, II, al. 3 de la loi 2004-575, qui fait référence aux articles 226-17, 226-21 et 226-22 du code pénal.

[158]Article 6, VI, 1 de la loi 2004-575.

[159]Les employés ne semblant pas entrer dans la catégorie du « public », sous réserve de la décision citée en note précédente. Dans le même sens voir CNIL, « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? », précité, dernière question, où la commission considère que « *les entreprises et les administrations fournissant un accès internet à leurs employés ne sont pas concernées par cette obligation de conservation* ».

[160]Voir supra notre note de bas de page n°3.

[161]Au delà du caractère jugé excessif, par une partie de la doctrine, de la réglementation relative à la conservation des données de trafic et de connexion. Voir par ex. Lionel Maurel, « Accès Internet en bibliothèque : ce qu'exige vraiment la loi », http://scinfolex.wordpress.com/2010/03/26/acces-internet-en-bibliotheque-ce-quexige-vraiment-la-loi/ ; Pearl Nasseripour, « Conservation des données personnelles : état des lieux », 9 août 2007, à propos du colloque « Conservation des données personnelles : état des lieux » qui s'est tenu le 29 juin 2007 à l'Université de Nanterre, http://www.e-juristes.org/Conservation-des-donnees/ ; Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, précitée en note n° 7, n° 770 et s. ; Groupe de travail « article 29 » sur la protection des données, avis 9/2004 du 9 nov. 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_fr.pdf. Plusieurs lois de transposition de la directive européenne sur la conservation des données ont par ailleurs soulevé des problèmes de constitutionnalité et de conformité à la Convention européenne des droits de l'Homme : voir par ex. « Atelier n°1 : Compétences transfrontalières en matière de cybercriminalité à l'ère de l'informatique dans les nuages », in *Les messages de Madrid*, EuroDIG 29-30 avril 2010, http://www.coe.int/t/informationsociety/documents/MsgsMadrid_fr.pd , p. 14.

[162]Voir supra, notre sous-titre 2.3 in « Surveillance, journalisation, analyse... ». Dans le même sens voir CNIL, « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? », précité, dernière question.

[163]Article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation des jeux d'argent et de hasard en ligne, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022204510. Voir également les décisions TGI Paris, référé, 6 août 2010, Autorité de régulation des jeux en ligne vs Neustar, Numéricable, Orange et a., http://www.legalis.net/spip.php?page=breves-article&id_article=2967 ; TGI Paris, référé, 28 avril 2011, Autorité de régulation des jeux en ligne vs Numéricable, Orange et a., http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3155.

d'atteinte à un droit d'auteur ou à un droit voisin[164], ou plus largement en cas de toute atteinte en ligne[165], lorsqu'il estime qu'une telle mesure est de nature à faire cesser cette atteinte.

En second lieu, les fournisseurs d'accès devront prochainement « *empêcher l'accès sans délai* » aux contenus contrevenant aux dispositions de l'article 227-23 du code pénal (relatif aux images et représentations de mineurs à caractère pornographique) dont les adresses leur seront notifiées par l'autorité administrative, aux termes du futur article 6, I, 7 alinéa 4 de la loi n° 2004-575. Cet alinéa, créé par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[166], dite LOPPSI 2, entrera en vigueur 6 mois après la publication de son décret d'application, et au plus tard à l'expiration d'un délai d'un an à compter de la publication de la loi[167].

Toutefois, notons que l'avocat général à la Cour de justice de l'Union européenne, dans l'affaire Scarlet Extended vs société belge des auteurs compositeurs et éditeurs (Sabam)[168], estime qu'une mesure de filtrage prononcée par un juge « *apparaît en réalité comme une "obligation" nouvelle de caractère général ayant vocation à être étendue, à terme, de manière permanente à tous les FAI* », et qu'elle ne présente donc pas les « *caractéristiques de concrétude et d'individualisation qui sont normalement attendues de toute riposte ou réaction à une conduite supposée spécifique et déterminée* »[169]. Une telle mesure, qui lui semble par ailleurs disproportionnée au regard des faits de violation de droits de propriété intellectuelle[170], est en effet « *appelée à affecter durablement un nombre indéterminé de personnes morales ou physiques, de FAI ou d'internautes, de prestataires de services de la société de l'information et d'utilisateurs desdits services* »[171]. Il en conclut qu'une telle mesure ne peut être mise en œuvre, à la lumière des principes de la Convention européenne des droits de l'Homme, que sur le fondement d'une base légale expresse et préalable[172], accessible, claire et prévisible[173], suffisamment précise quant aux garanties offertes à l'individu contre l'arbitraire[174]. Il considère enfin que la loi belge permettant au juge de prononcer une mesure de filtrage dans l'affaire qui lui est soumise ne répond pas à ces critères[175]. Une lecture similaire pourrait être faite des lois françaises[176].

3.3 Obligations d'information et de mise en place de dispositifs de signalement ?

Les FAI voire les opérateurs ont enfin plusieurs obligations d'information et de mise en place de dispositifs de signalement, qui ne concernent a priori pas les établissements publics d'enseignement supérieur, sous réserve toutefois de ce que pourrait décider la jurisprudence de leur statut, compte tenu de l'arrêt de la Cour d'appel de Paris du 4 février 2005[177].

Il s'agit en premier lieu d'une obligation d'information sur l'existence de moyens de filtrage. L'article 6, I de la loi n° 2004-575 dispose que les FAI doivent informer leurs abonnés de « *l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner* » et leur proposer « *au moins un de ces moyens* ». Ils doivent encore les informer « *de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation (de vigilance) définie à l'article L. 336-3* » du CPI[178], et leur proposer « *au moins l'un des moyens figurant sur la liste prévue* » à l'article L. 331-26 du même code.

Il s'agit en deuxième lieu d'une obligation d'information sur les risques et moyens de protection associés à l'utilisation des services de communications électroniques, à la charge des opérateurs. L'article L. 121-83-1 du code de la consommation, créé par l'ordonnance n°2011-1012 du 24 août 2011 leur fait en effet obligation de mettre « *à la disposition des consommateurs et (de tenir) à*

[164]Article 336-2 du CPI, tel que modifié par la loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite « Hadopi 1 », précitée. Le juge se prononce à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits visées à l'article L. 321-1 du CPI ou des organismes de défense professionnelle visés à l'article L. 331-1 de ce code.

[165]Article 6, I, 8 de la loi n° 2004-575, et plus largement article 809 du code de procédure civile.

[166]Loi accessible sur le site de Légifrance (http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9EECCF8D81F16BED397A1BAEE624EA1A.tpdjo12v_2?cidTexte=JORFTEXT000023707312&dateTexte=20111019), article 4.

[167]Article 4 de la loi.

[168]Conclusions de l'avocat général M. Pedro Cruz Villalón présentées le 14 avril 2011 dans l'affaire C-70/10, Scarlet Extended SA contre Société belge des auteurs compositeurs (Sabam) et autres, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=fr&num=79889585C19100070&doc=T&ouvert=T&seance=CONCL. Voir également le communiqué de presse n° 37/11 de la Cour de Justice relatif à ces conclusions en date du 14 avril 2011, http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037fr.pdf.

[169]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 66.

[170]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 68.

[171]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 62.

[172]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 105.

[173]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 96. Il précise que ces conditions d'accessibilité, de clarté et de prévisibilité « *découlent (toutes) de l'idée de prééminence du droit* » consacré par le préambule de la Conv. EDH, tel qu'il le rappelle en son §100.

[174]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, § n° 95.

[175]Conclusions de l'avocat général M. Pedro Cruz Villalón, précitées, §§ n° 105, 108.

[176]Pour une analyse des mesures de filtrage à la lumière des principes de la Conv.. EDH, voir Cormac Callanan, Marco Gercke, Estelle De Marco, Hein Dries-Ziekenheiner, *Filtrage d'Internet - Equilibrer les réponses à la cybercriminalité dans une société démocratique* , traduction française du 20/05/2010, juriscom.net, http://www.juriscom.net/actu/visu.php?ID=1227.

[177]Voir supra notre note de bas de page n°3.

[178]Voir supra, notre sous-titre 2.1.2.2.

jour dans ses points de vente et par un moyen téléphonique ou électronique accessible en temps réel à un tarif raisonnable » plusieurs types d'information, et notamment des informations sur « *les conséquences juridiques de l'utilisation des services de communications électroniques pour se livrer à des activités illicites ou diffuser des contenus préjudiciables, en particulier lorsqu'ils peuvent porter atteinte au respect des droits et des libertés d'autrui, y compris les atteintes aux droits d'auteur et aux droits voisins* », et sur « *les moyens de protection contre les risques d'atteinte à la sécurité individuelle, à la vie privée et aux données à caractère personnel lors de l'utilisation des services de communications électroniques* ».

Il s'agit enfin d'une obligation, à la charge des FAI, de mettre en place des dispositifs de signalement et de contribuer activement à la lutte contre les contenus illicites. L'article 6, I, 7 al. 3 de la loi n°2004-575 impose tout d'abord à ces prestataires de « *mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance* » divers types de contenus en ligne (atteintes volontaires à la vie ou à l'intégrité physique, provocation à la haine raciale, pédopornographie, contenu violent susceptible d'être vu par un mineur...)[179], « *d'informer promptement* » les autorités compétentes des activités illicites entrant dans ces catégories qui leur seraient signalées, et de « *rendre publics les moyens (qu'ils) consacrent à la lutte contre ces activités illicites* »[180]. L'article 6, I, 7, al. 7 de cette même loi de 2004[181] impose en second lieu aux FAI de mettre « *en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes* » en matière d'activités illégales de jeux d'argent. Ils doivent également informer « *leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi* »[182].

Conclusion

Ce panorama des différents droits et obligations qu'ont les établissements publics d'enseignement supérieur dans le cadre des accès réseaux qu'ils organisent au bénéfice de leurs étudiants, de leur personnel et de visiteurs, nous montre que ces droits et obligations peuvent finalement être répartis en deux catégories : ceux dont l'application est plutôt certaine, et celle dont l'application est plutôt incertaine, laissant les établissements dans une insécurité juridique bien souvent partagée par d'autres acteurs, tels que les entreprises du secteur privé.

Dans la première de ces catégories, figure notamment l'obligation de respecter le RGS[183], tout du moins pour toutes les fonctions du système d'information susceptibles d'être utilisées pour échanger des informations avec les utilisateurs ou d'autres administrations, et pour traiter et conserver ces informations. Le contenu de ce RGS correspond par ailleurs à un certain état de l'art dont le non respect pourrait sans doute être reproché à un établissement par un juge, y compris si le dommage allégué par la victime n'a pas pris place dans le cadre de relations entre l'établissement et ses usagers ou d'autres administrations[184]. Figurent encore dans cette catégorie diverses obligations de sécurisation, comme celle relative aux traitements de données à caractère personnel[185], l'obligation de filtrer sur ordonnance du juge ou, à l'avenir, sur demande de l'autorité administrative[186], et l'obligation de conserver les données d'identification et de trafic des étudiants et visiteurs utilisant Internet ou le réseau local si ce dernier peut-être considéré comme ouvert « au public »[187], sachant que si cette obligation est moins certaine concernant les employés, un droit de conserver certaines données pour des raisons de « contrôle employeur » leur est également accordé, sous réserve de prendre certaines précautions[188]. Figure enfin dans cette liste l'obligation de préserver le secret des correspondances, a minima sur la base des règles pénales et civiles traditionnelles, et le droit de prendre certaines autres mesures en vue de préserver les intérêts de l'établissement et notamment de renforcer sa sécurité juridique, qui passe entre autres par le droit de conserver certaines données techniques pour des raisons de sécurité[189], d'organiser l'utilisation des ressources informatiques dans le cadre notamment de la rédaction de chartes ou de filtrer certains contenus, en faisant toutefois dans ce dernier cas preuve de prudence[190].

Dans la seconde catégorie, celle des obligations incertaines, nous pouvons inclure la plupart des autres obligations mises à la charge des FAI et des opérateurs, par exemple leur obligation d'information et de mise en place de dispositifs de signalement dans

[179]Sur les doutes pouvant persister s'agissant des infractions visées par cette obligation, voir Estelle De Marco, *L'anonymat sur Internet et le droit*, thèse, précitée en note n°7, n° 803 et suivants.

[180]Article 6, I, 7, al. 8 de la loi n° 2004-575. Le non respect de cette obligation est puni d'un an d'emprisonnement et de 75 000 euros d'amende.

[181]Alinéa inséré par l'art. 40 de la loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, JORF n° 56 du 7 mars 2007 p. 4297, texte n°1, http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CC8464AB0F18D8117EDD07665CE3F907.tpdjo12v_2?cidTexte=JORFTEXT000000615568&dateTexte=20111019.

[182]Article 6, I, 7, al. 8 de la loi n° 2004-575. Le non respect de cette obligation est puni d'un an d'emprisonnement et de 75 000 euros d'amende.

[183]Voir supra, notre sous-titre 2.1.1.1.

[184]Voir supra, notre sous-titre 2.2.2. notamment sous « responsabilité administrative ».

[185]Voir supra, notre sous-titre 2.1.2.1.

[186]Voir supra, notre sous-titre 3.2.

[187]Voir supra, notre sous-titre 3.1. Sur la notion de « public », voir notre titre 1 et notre note n° 11.

[188]Voir supra, notre sous-titre 2.3, sous « Surveillance, journalisation, analyse... ».

[189]Voir supra, notre sous-titre 2.3, sous « Surveillance, journalisation, analyse... ».

[190]Voir supra, notre sous-titre 2.3, respectivement sous « Chartes » et sous « filtrage ».

le cadre de la lutte contre les contenus illicites[191], et leur obligation de préserver l'intégrité et la sécurité des réseaux[192], même si la mise en œuvre de cette dernière obligation présente un intérêt certain pour un établissement, qu'elle est susceptible de renforcer sa sécurité juridique et qu'elle est du moins en partie obligatoire en application des règles du RGS. Peuvent encore être incluses dans cette catégorie l'obligation de notification d'une violation de données personnelles à la CNIL, malgré les sanctions très lourdes attachées à une absence de notification[193], et les modalités selon lesquelles l'obligation de l'article 335-5 du CPI[194] peut-être respectée, en l'absence de moyens de sécurisation labellisés ou si ces moyens se révélaient dans le futur incompatibles avec les systèmes d'information des établissements. Ces incertitudes touchant plus largement l'ensemble des entreprises et parfois les particuliers, il convient d'espérer qu'elles reçoivent une réponse plus certaine dans un proche avenir.

[191]Voir supra, notre sous-titre 3.3.

[192]Voir supra, notre sous-titre 2.1.1.2.

[193]Voir supra, notre sous-titre 2.1.2.1.

[194]Voir supra, notre sous-titre 2.1.2.2.