MISSION DE RECHERCHE
DROIT & JUSTICE

Synthèse

Étude de droit comparé en matière d'organismes de contrôle des interceptions de télécommunication

Réalisée par Claudine Guerrier

Professeur

Télécom et Management SudParis

Janvier 2009

Département de droit, économie, finances et sociologie

« les organismes de contrôle des interceptions de télécommunication»

NOTE DE SYNTHESE

Les interceptions légales sont des dérogations au secret des correspondances et au respect de la vie privée. La Déclaration universelle des droits de l'homme de 1948[1] est une référence incontournable, même si elle n'est pas toujours appliquée. L'article 17 du pacte international relatif aux droits civils et politiques des Nations unies du 16 décembre 1966 reprend les mêmes notions sous une présentation quasi identique[2]. Ces deux textes d'inspirent du cercle privé.
Le droit français mentionne le respect de la vie privée dans l'article 9 du Code civil et dans la loi du 17 juillet 1970, soucieuse de renforcer la protection des libertés individuelles. La Convention européenne des droits de l'homme, à travers son article huit, donne une légitimité à la sphère privée.
Les interceptions légales de télécommunications ou de communications électroniques[3] s'appliquent à la téléphonie fixe, à la téléphonie mobile, à l'Internet.
L'objectif des Etats-nations est de parvenir à un équilibre difficile entre la sécurité et la protection de la vie privée. Les organismes de contrôle jouent un rôle privilégié dans cette problématique.
Les interceptions de télécommunication, dans les Etats occidentaux ont connu deux phases distinctes : la première tend à limiter le nombre des interceptions de télécommunication ; elle établit des organismes de contrôle ; elle correspond aux deux dernières décennies du vingtième siècle. La deuxième s'inscrit dans le courant sécuritaire qui recourt à la vidéosurveillance, à la biométrie. Les personnes publiques utilisent de plus en plus fréquemment les interceptions de télécommunication. Cependant, les organismes de contrôle subsistent ; ils constituent l'un des rares freins à l'idéologie sécuritaire qui se manifeste à la fin du vingtième siècle et au début du vingt-et-unième siècle. Une problématique secondaire s'attache à une étude de droit comparé entre interceptions judiciaires et interceptions de sécurité, les motifs d'interception et les organismes de contrôle, les données techniques et les organismes de contrôle.

La première partie du rapport correspond à la problématique Sécurité/ Vie privée.
Les organismes de contrôle ont été mis en place en Europe à l'initiative de la CEDH, qui applique la Convention européenne des droits de l'homme. Aux USA, c'est la culture juridique fédérale qui est prise en compte.
En ce qui concerne la CEDH, il convient de citer l'arrêt Klass[4], l'arrêt Malone[5], les arrêts Kruslin et Huvig[6]. Dans les arrêts Malone, Kruslin, Huvig, la CEDH enjoint aux Etats de revoir leur législation pour se conformer au droit humanitaire, instituer un ou deux organismes de contrôle.
Aux USA, les interceptions fédérales sont l' »Omnibus Crime Control and Safe Streetss Act »,

[1] L'article 12 de la Déclaration universelle des droits de l'homme du 12 décembre 1948 précise : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions »
[2] L'article 17 du 16 décembre 1966 :
« 1.Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.
2.Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »
[3] Union européenne ; directives du 7 mars 2002
[4] CEDH, Affaire Klass et autres c.RFA, 6 septembre 1978
[5] CEDH Malone c.Royaume-Uni, 2 août 1984
[6] CEDH, Kruslin c.France, Epoux Huvig c.France, 24 avril 1990

Title III, adopté en 1968, la FISA[7], la CALEA, de 1994.Cette dernière devait permettre de faire face aux rapides mutations des technologies de télécommunications, affirmer l'obligation pour les opérateurs de télécommunications de prêter leur concours aux services autorisés à procéder à des interceptions de communications et à des identifications d'appel. La FISA, quant à elle, est l'une des conséquences législatives de l'affaire du Watergate survenue quelques années auparavant dans un domaine éminemment sensible qui était jusqu'alors régi par les « Executive orders ». Lorsque les juges de la Cour spécifique instituée par le FISA Act ont approuvé leur demande, ils donnent l'ordre à l'opérateur d'exécuter matériellement la décision. En cas d'urgence, l'Attorney General, ou son délégué est habilité à autoriser une interception, à condition que les juges soient prévenus et qu'une régularisation intervienne dans un délai de 24 heures. L'Attorney General, premier responsable des mesures d'autorisation, est tenu de faire parvenir chaque année un rapport à l'administration des tribunaux fédéraux et au Congrès sur l'application de la FISA.

Au Royaume-Uni, après l'arrêt Malone, la loi de 1985 « The Interception of Communication Act » confie au ministre de l'Intérieur la responsabilité de délivrer l'autorisation d'interception. Les interceptions sont administratives. Le contrôle est effectué d'une part, par le « Commissioner », une personne désignée par le Premier ministre qui a pour mission de contrôler si l'exécutif exerce ses prérogatives en conformité avec la loi, d'autre part par l'Interception of Communication Tribunal, dont les membres sont désignés pour une durée de cinq ans.

En Allemagne, les interceptions sont judiciaires et de sécurité. La législation existait en RFA depuis le 13 août 1968. Les interceptions judiciaires sont décidées par le juge d'instruction. En cas d'urgence, le Procureur est habilité à prendre la décision d'interception, à condition que la dite décision soit confirmée par le juge d'instruction dans les trois jours. Les interceptions de sécurité sont autorisées par des personnalités exerçant un pouvoir exécutif. La loi de 1968 a été complétée à plusieurs reprises : en 1978, obligation est faite, après l'expiration de la mesure d'informer la personne qui en a été l'objet, à condition de ne pas compromettre la finalité poursuivie ; en 1989, tous les opérateurs sont tenus de participer aux mesures d'interception. Le contrôle est effectué par deux commissions, le PKG et la commission G10. La loi de 1997 met davantage l'accent sur la sécurité. Elle autorise les juges allemands à procéder à des interceptions de conversation à distance et à des interceptions dans les logements privés pour les enquêtes judiciaires, quand il s'agit de faits particulièrement graves.

En Espagne, le secret des correspondances est garanti par l'article 18.3 de la Constitution[8] mais, aux termes de l'article 55, alinéas un et deux de la Constitution, le secret des communications peut être suspendu lorsque l'état d'exception ou de siège est proclamé en vertu d'une loi organique réprimant l'activité des bandes armées ou de mouvements terroristes. Les autorisations d'interceptions de télécommunications sont octroyées, par écrit, sous forme motivée, par l'autorité judiciaire compétente. En cas d'urgence, la mesure est prise par le ministre de l'Intérieur, le directeur de la sûreté de l'Etat : le juge est informé par écrit. Il rapporte ou conforme la décision dans un délai maximal de 72 heures. Le résultat de l'interception doit être communiqué régulièrement au juge, qui est en mesure de rapporter la décision à tout moment.

L'Italie a un régime mixte, avec interceptions judiciaires et interceptions de sécurité. Le code pénal permet au Parquet, après autorisation préalable du juge compétent, d'intercepter les télécommunications, pour des délits énumérés. La durée légale des interceptions n'excède pas quinze jours ; l'interception est toutefois renouvelable, elle peut être prorogée par le juge par période de quinze jours. Les interceptions de sécurité sont autorisées par le ministre de l'Intérieur.

[7] Foreign Intelligence Surveillance Act

[8] Est garanti le secret des communications, spécialement par poste, télégraphe et téléphone, exception faite du mandat judiciaire

En Belgique, l'inviolabilité des communications était consacrée par la loi du 13 octobre 1930, tandis que l'article 90 ter D du Code d'instruction criminelle inséré dans la loi du 30 juin 1994 stipule que le juge d'instruction peut autoriser les communications moyennant le respect de conditions : intervention du juge d'instruction, respect du principe de proportionnalité, limitation dans le temps de la mesure[9]. Un contrôle parlementaire existe : chaque année, un rapport est remis au Parlement au sujet de l'application des dispositions relatives à l'interception des communications et télécommunications privées. L'interception de sécurité correspond à l'interception militaire, effectuée par le service général du renseignement et de la sécurité des forces armées.
En France, les interceptions sont judiciaires et de sécurité. Les lois sur les interceptions de télécommunications sont la loi du 10 juillet 1991 et la loi du 9 mars 2004. L'interception judiciaire au stade de l'instruction est autorisée, jusqu'en 2009, par le mandat du juge d'instruction, sur la base du quantum de la peine[10], pour une durée de quatre mois, renouvelable. La réforme annoncée des juges d'instruction va induire des modifications qui ne sont pas connues. Les interceptions de sécurité sont demandées par des services et notamment par des services de renseignement du ministère de la Défense, du ministère de l'Intérieur, du ministre en charge des Douanes, autorisées par le Premier ministre, chef de l'administration qui travaille sur ce point avec des délégués. Les interceptions de sécurité sont autorisées pour des raisons limitativement énumérées : atteinte à la sécurité nationale, prévention des actes de terrorisme, prévention de certains crimes et délits, atteinte au patrimoine scientifique et économique. Un organisme de contrôle est créé : il s'agit de la CNCIS, commission nationale de contrôle des interceptions de sécurité, autorité administrative indépendante, composé d'un président, désigné par le président de la République, d'un député, désigné par le président de l'Assemblée nationale, d'un sénateur, désigné par le président du Sénat. La CNCIS contrôle la conformité des motifs et donne un avis, favorable ou défavorable, auquel le premier ministre peut passer outre. Elle réalise des inspections. Elle établit un rapport annuel, qui est rendu public. Elle peut être saisie par des particuliers et procède alors à des vérifications.

Avec la fin du vingtième siècle, et le début du vingt-et-unième siècle, les nouvelles technologies se développent et la tentation sécuritaire s'accroît : il est si facile d'intercepter, de stocker, de conserver…Avec l'essor des moyens sophistiqués et globalisés de communication et d'information, les Etats veulent s'assurer d'une sécurité toujours plus prégnante. Les attentats qui ont lieu aux USA, c'est-à-dire dans la seule puissance disposant d'un rayonnement géo-politique mondial, sont largement médiatisés et semblent justifier, aux yeux de l'opinion publique, une lutte contre le terrorisme, mais aussi contre toutes les formes d'anti-conformisme. Les organismes de contrôle, à quelques exceptions près sont moins influents, plus prudents.
Aux USA, le Patriot Act[11] apporte des modifications au droit américain pour augmenter la capacité qu'ont les agents de police d'obtenir certains types de mandats des tribunaux afin d'intercepter les communications et pour accroître les catégories d'informations que ces mandats permettent d'obtenir dans certaines circonstances.
En 2002, le président Bush signe un décret-loi secret autorisant la National Security Agency, l'organisme chargé de l'interception de renseignements étrangers d'origine électromagnétique aux USA, à surveiller et à intercepter les appels téléphoniques effectués et les courriels internationaux transmis par des personnes aux USA à des personnes à l'extérieur des USA et inversement, sans avoir à solliciter une autorisation judiciaire préalable du tribunal de la FISA.
Le 17 janvier 2006, deux poursuites distinctes sont déposées contre le programme de surveillance sans mandat de la NSA, la première par un groupement d'organismes de protection des libertés

[9] Un mois renouvelable avec une durée maximale de six mois
[10] Deux ans d'emprisonnement
[11] En Octobre 2001

individuelles dirigées par l'ACLU[12], le deuxième par le Center for Constitutional Rights (CCR) contre le président Bush, la NSA, et le Federal Bureau of Investigation (FBI). La justice s'est prononcée deux fois. En août 2006, la juge fédérale Anna Diggs Taylor, siégeant à Chicago, avait validé une plainte déposée par des avocats, des journalistes, des enseignants, qui se trouvaient en contact fréquent avec le Proche-Orient et qui estimaient que leurs communications étaient sous surveillance. Considérant que le président George W.Bush avait outrepassé ses pouvoirs en autorisant le programme, elle avait exigé sa fin immédiate. Un appel a été déposé et la décision de la juge Diggs Taylor a été suspendue en attendant que la Cour d'appel se prononce. En juillet 2007, l'ordre d'arrêter les interceptions « antiterroristes » aux USA sans mandat d'un juge a été annulé par une Cour d'appel fédérale.
Une loi promulguée le 5 août 2007 réforme la FISA. Elle est seulement valable pour six mois. La loi FISA de 2008 se substitue au texte de 2007 ; elle a été adoptée définitivement par la Chambre des Représentants le 20 juin 2008 et par le Sénat le 10 juillet 2008 par 69 voix (dont celle de M.Obama) contre 28. La loi permet d'obtenir un mandat d'un an pour des interceptions de groupes et d'individus étrangers. Un Américain peut, quant à lui, être intercepté si la communication concerne l'étranger. Les autorités disposent à présent d'une semaine, et non de 72 heures pour obtenir un mandat. Elles doivent avoir l'aval du tribunal spécial instauré par la loi pour intercepter les conversations d'un Américain à l'étranger, alors qu'avant l'approbation du ministre de la justice suffisait. La loi accorde en outre l'immunité juridique aux opérateurs de télécommunications américains accusés par la justice américaine de collaborer avec le gouvernement et les services secrets afin de pratiquer des interceptions illégales. En 2008, malgré l'arrêt de la Cour d'appel fédérale mentionné ci-dessus, une quarantaine de requêtes en recouvrement de plusieurs milliards de dollars ont été engagées dans le cadre d'interceptions téléphoniques aux USA. Le projet initial ne mentionnait pas l'immunité juridique. Cette dernière est essentielle pour l'Exécutif et pour les opérateurs de télécommunications.
Au Royaume-Uni, entre en vigueur en Octobre 2000 la Regulation of Investigatory Powers Act[13], qui se substitue à l'Interceptions of Communications Act 1985. La RIPA englobe les diverses technologies de télécommunications. Il s'agit de réaliser un équilibre entre les pouvoirs d'enquête des organisations habilitées, opérateurs et fournisseurs, et le souci de protection des droits de l'homme, en particulier la vie privée. Les mandats pour intercepter une communication sont délivrés par le secrétaire d'Etat à l'Intérieur, ou, en cas d'urgence, par un cadre supérieur du gouvernement et soumis à la surveillance d'un « Interceptions of Communications Commissioner ». Le « Anti-Terrorism, Crime and Security Act » de décembre 2001 porte la durée de conservation des données de connexion des internautes par les fournisseurs d'accès à un an au moins.
En Allemagne, la réunification de la RFA et de la RDA ne s'est pas accompagnée d'une libéralisation de la norme en matière d'interceptions de télécommunications. La loi sur les télécommunications de juillet 1996 exige des fournisseurs d'accès à Internet de rendre possible la consultation des données du trafic Internet par les services secrets. En 2001, la loi G10 est amendée : il est demandé aux opérateurs et aux fournisseurs d'accès de mettre tout en œuvre pour permettre aux services de renseignement de surveiller ou d'intercepter les communications électroniques, nationales et internationales. Cependant, en février 2007, la Cour fédérale de justice refuse à la police le droit de fouiller en secret à distance, via Internet, les disques durs de personnes soupçonnées de terrorisme. Elle définit un droit fondamental à la protection de la confidentialité et de l'intégrité des systèmes informatiques.
En Belgique, une commission permanente chargée du suivi du comité R est créée en 1999 ; elle se substitue à la commission spéciale qui avait été mise en place auparavant. Le comité R approuve en 2001 un projet de loi qui élargit l'exception existante pour le service général du

[12] Tribunal fédéral de district de Détroit
[13] RIPA

renseignement et de la sécurité des forces armées. Les interceptions de sécurité sont prises en compte au début du 21ème siècle dans le cadre de la lutte contre le terrorisme et la criminalité organisée. En 2007, est déposé un projet de loi afférent aux méthodes de recherche pour les services de renseignement.
En Espagne, le 27 juin 2002, le Congrès des députés espagnols adopte la loi de l'Internet[14], qui oblige les fournisseurs d'accès à Internet à conserver les données de connexion et de trafic de leurs clients pendant au moins un an.
En Italie, la loi 374 du 18 octobre 2001 considère comme un crime le simple fait de participer à toute activité préparatoire, en association avec d'autres personnes dans le but d'accomplir des actes de terrorisme. En particulier, il étend l'application de ce régime aux interceptions téléphoniques légales.
En France, la loi du 23 janvier 2006 est relative à la lutte contre le terrorisme : afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités soit des services de police soit de gendarmerie nationale spécialement chargés de ces tâches peuvent exiger des fournisseurs la communication des données conservées et traitées. Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée, désignée par la CNCIS sur proposition du ministre de l'Intérieur.
En Suède, le 18 juin 2008, le Parlement suédois adopte[15] une loi qui autorise l'Agence d'écoutes militaires suédoise à intercepter les méls et les communications téléphoniques entrant et sortant du pays ; deux commissions de contrôle sont néanmoins chargées de procéder à la surveillance des interceptions.
D'une façon générale, ces organismes de contrôle ont moins de pouvoir et l'équilibre penche en faveur de la sécurité.

La deuxième partie correspond aux problématiques secondaires.Les problématiques secondaires concernent les motifs d'interceptions et les interceptions techniques.
Les motifs intéressent aussi bien les interceptions judiciaires que les interceptions de sécurité.
En Allemagne, les interceptions sont possibles si la personne ciblée a commis des crimes comme l'assassinat, l'homicide volontaire, des délits au regard de la sécurité de l'Etat, la haute trahison, l'atteinte à la sûreté extérieure de l'Etat, l'espionnage, l'association de malfaiteurs. La prise en compte des formes récentes de l'insécurité en Europe a conduit à l'élargissement des motifs justifiant le recours au contrôle stratégique, c'est-à-dire à la surveillance exercée sur certaines liaisons entre l'Allemagne et l'étranger. Le Conseil constitutionnel fédéral dans un arrêt du 14 juillet 1999 a déclaré que les dispositions portant sur les diverses formes de contrôle stratégiques insérées dans la loi en 1994 étaient en grande partie incompatibles avec la Constitution, sans pour autant déclarer que ce type de surveillance était illicite.
En Italie, le code de procédure pénal autorise les interceptions pour le trafic d'armes, la contrebande, mais aussi pour les injures, les menaces, molestations ou troubles à la personne par le biais du téléphone.
En Espagne, les motifs invoqués à l'appui d'interceptions de communications électroniques peuvent avoir deux fondements. Le premier correspond aux alinéas un et deux de l'article 55 de la Constitution selon lesquels le secret des communications peut être suspendu lorsque l'état d'exception ou de siège est proclamé en vertu d'une loi organique réprimant l'activité des bandes armées ou de mouvements terroristes. Par ailleurs, la loi anti-terroriste espagnole du premier décembre 1980 réserve la surveillance des communications à la prévention ou à la répression des activités délictueuses de bandes armées ou d'éléments terroristes. Ces activités comprennent les délits contre la vie et l'intégrité physique, les détentions illégales sous menace de rançon, la possession ou la détention d'armes, munitions, explosifs, l'atteinte à la sûreté de l'Etat.

[14] LSSICE
[15] A une courte majorité : 143 voix pour, 138 contre, une abstention

Aux USA, le « Title III Act » (correspondant aux interceptions judiciaires) autorise les interceptions de télécommunications effectuées lors des enquêtes criminelles, quand il s'agit d'infractions graves, c'est-à-dire des meurtres, kidnappings, affaires de drogues ainsi que toutes les actions « qui attentent à la vie, à l'intégrité physique ou à la propriété, et qui sont punissables d'une peine d'emprisonnement d'au moins un an ».
Le FISA Act concerne la surveillance des télécommunications effectuées dans le secteur des activités de renseignement d'une puissance étrangère, celles qui sont nécessaires à la protection de la sécurité de l'Etat pour les motifs suivants : attaques contre le pays, effectives ou avérées, actes de sabotage, terrorisme international, activités subversives au profit des services de renseignement d'une puissance étrangère.
En Belgique, les interceptions judiciaires sont limitées à un petit nombre de motifs : grande criminalité, terrorisme, grand banditisme, crime organisé. Les interceptions de sécurité sont afférentes à la sécurité nationale et des forces armées.
En France, en matière d'interceptions judiciaires, au stade de l'instruction, la notion de motif n'est pas retenue. C'est le quantum de la peine[16]qui est retenu. En matière d'enquêtes préliminaires, introduites par la loi Perben deux, les motifs sont les suivants : meurtre commis en bande organisée, tortures et actes de barbarie commis en bande organisée, trafic de stupéfiants, enlèvement et séquestration commis en bande organisée, traite des êtres humains, proxénétisme, vol commis en bande organisée, extorsion, destruction, dégradation et détérioration d'un bien commis en bande organisée, faux monnayage, crimes et délits constituant des actes de terrorisme, délits en matière d'armes commis en bande organisée, aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée, délits de blanchiment ou de recel, association de malfaiteurs. En matière d'interceptions de sécurité, les motifs sont prévus dans la loi du 10 juillet 1991 : sécurité nationale, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisée, de la reconstitution ou du maintien de groupements dissous, protection des éléments essentiels du potentiel scientifique et économique de la France.
Aux Pays-Bas, l'interception judiciaire est possible en cas de flagrant délit ou en cas de délit pour lequel la détention préventive est autorisée[17].
Au Royaume-Uni, la loi stipule que les interceptions sont possibles pour l'intérêt de la sécurité nationale, pour la prévention ou la découverte d'un crime grave, pour la sauvegarde de la prospérité économique du Royaume-Uni.
Ainsi, il apparaît que la motivation, en matière d'interceptions judiciaires correspond la plupart du temps à des crimes et aussi à des délits dont la gravité varie avec la culture juridique du pays. Dans le domaine des interceptions de sécurité, les motifs sont le plus souvent relatifs à la sécurité extérieure ou intérieure des Etats.

Quant aux interceptions de données techniques, elles apparaissent avec le développement d'Internet.
Au niveau de l'Union européenne, la directive dénommée « Data Retention » permet en 2006 de conserver les paramètres techniques pendant une durée qui va de six à vingt-quatre mois. Cette directive est intervenue après l'adoption du projet de décision-cadre par le Conseil européen les 29 et 30 avril 2004, sur l'initiative de quatre pays, la France, l'Irlande, le Royaume-Uni, la Suède. Ce texte envisage une durée de conservation minimale fixée à un an, susceptible d'être portée à trois ans. Ces données concernent les appels, les SMS, les méls effectués par les abonnés. La directive s'appuie sur le projet de décision-cadre.
Au niveau national, des durées ont été fixées pour les données techniques. En la matière, le Royaume-Uni a joué un rôle d'avant-garde ; la Cour constitutionnelle de Karlsruhe a pris en

[16] Deux ans
[17] Article 125 f du code de procédure pénale

compte les libertés individuelles ; en France, le législateur a progressivement mis l'accent sur davantage de sécurité.
Au Royaume-Uni, la RIPA prend en compte l'importance d'Internet et les méthodes de chiffrage qualifiées de solides. La RIPA peut être invoquée pour des motifs tenant à la sécurité nationale, à la prévention des crimes et des troubles à l'ordre public, à la protection de la santé publique et de la santé économique du pays. La RIPA permet :

- d'exiger, dans le secret, qu'un FAI lui donne accès aux communications d'une personne
- la surveillance de l'ensemble des communications électroniques transitant par le territoire britannique
- de demander à un fournisseur d'accès de mettre à niveau ses équipements de télécommunications afin de faciliter la surveillance
- pour le gouvernement d'exiger qu'une personne lui remette les clés ayant servi à chiffrer ses informations

Le « Anti-Terrorism, Crime and Security Act » a porté au Royaume-Uni la durée de conservation des données de connexion des internautes par les fournisseurs d'accès à un an au moins. Le contrôle s'amenuise : la police est dispensée en de multiples occasions de l'autorisation préalable d'un juge. Il suffit d'obtenir l'accord du ministre de l'Intérieur ou l'un de ses proches collaborateurs pour agir.
En Allemagne, le 24 mai 2007, le Bundestag adopte la loi « anti hacker » en débattant notamment sur les paragraphes 202 et 303. Le paragraphe 202 prohibe l'accès non autorisé à des données informatiques de l'Etat et des entreprises, en particulier le contournement de mesures techniques de protection des données. Le 4 juillet 2007, le Bundestag adopte la loi sur la propriété intellectuelle. Un amendement fait de l'échange de fichiers par les réseaux P2P une infraction passible d'une contravention. Le 10 novembre 2007, le Bundestag adopte[18]la loi qui transpose la directive « Data Retention ». Le premier janvier 2008, la loi impose aux opérateurs de téléphonie fixe et mobile de stocker les numéros de téléphone, date et heure des échanges ou lieu de l'appel. Depuis le premier janvier 2009, les fournisseurs d'accès à Internet sont astreints à la même obligation pour ce qui concerne la conservation des adresses IP et des logs de connexion. La Cour constitutionnelle de Karlsruhe a rendu une décision préliminaire le 19 mars 2008. Cette décision n'exclut pas le principe de conservation des données de connexion mais limite néanmoins l'utilisation de ces données de connexion à des délits et des crimes graves, homicides, abus sexuels, affaires de terrorisme, affaires de fraude fiscale ou de corruption et à condition que la demande d'accès aux données intervienne dans le cadre d'une procédure judiciaire. Les sociétés d'auteurs ou de producteurs de cinéma ou de musique ne peuvent pas utiliser ces données afin de lutter contre le piratage sur Internet.
En France, le décret du 24 mars 2006[19] n'englobe pas toutes les situations légales où la conservation est prévue. Ainsi, le décret laisse de côté les hypothèses où la conservation est liée à l'application de la LCEN. La loi du 23 janvier 2006 n'est pas expressément visée par le décret mais l'article L34-1-1 de cette loi renvoie à l'article L34-1 pour ce qui est des personnes soumises à la conservation et pour les catégories de données qui doivent être communiquées aux agents habilités. L'article R 10612 du CPCE, créé par le décret, définit les données relatives au trafic mais uniquement pour l'application des II et III de l'article L 34-1 du CPCE et non pour l'ensemble des cas où cette conservation peut être requise. Les données qui doivent être conservées sont les informations permettant d'identifier l'utilisateur, les données afférentes 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

[18] Par 366 voix contre 156
[19] Après l'adoption de la loi sur la sécurité quotidienne, la loi pour la confiance dans l'économie numérique, la loi anti-terrorisme

complémentaires demandés ou utilisés et leurs fournisseurs, les données susceptibles d'identifier le ou les destinataires de la communication, les données susceptibles d'identifier l'origine et la localisation de la communication. Une durée fixe d'un an est assignée à la conservation des données afférentes au trafic lorsqu'il s'agit de la recherche, de la constatation, de la poursuite des infractions. Cette durée ne peut être réduite et commence à courir à compter de l'enregistrement des données. Une durée fixe d'un an est assignée à la conservation des données afférentes lorsqu'il s'agit de la facturation, du paiement des créances. Une durée maximale de trois mois est assignée à la conservation des données relatives à la sécurité des réseaux et des installations. Les opérateurs de communications électroniques et les fournisseurs d'accès ne sont pas les seules personnes concernées par ce décret sur la conservation des données de connexion. Les personnes qui, au titre d'une activité professionnelle accessoire, fournissent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau. Tel est notamment le cas des cybercafés. Un autre décret d'application est relatif à la LCEN et à son article six. Officiellement, les données ne servent qu'à permettre l'identification de quiconque a contribué à la création du contenu du service, mais, en fait, le décret prévoit la conservation de nombreuses données, y compris le mot de passe fourni lors de la souscription d'un contrat d'abonnement ou lors de la création d'un compte auprès du prestataire Internet. Le décret[20] détermine à quelles conditions les services de police et de gendarmerie peuvent demander et traiter les données conservées par les fournisseurs d'accès et d'hébergement. Ce chapitre indique que les données, une fois obtenues, pourront être conservées pendant une durée de trois ans.
Les données techniques jouent aussi un rôle important dans le droit de la propriété intellectuelle. Pour la CNIL, comme pour la Commission de Bruxelles, les adresses IP sont des données personnelles. La décision du Conseil d'Etat annulant la décision de la CNIL du 18 octobre 2005 autorise la collecte d'adresses IP dans le cadre de la lutte contre les téléchargements illégaux ; ainsi, des constats de contrefaçon sont-ils effectués et les adresses IP associées sont conservées. La loi « Création et Internet » prévoit que le rapprochement entre les adresses IP et l'identité des titulaires de lignes peut être effectué par les fournisseurs d'accès Internet à la demande de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet, et non plus seulement du juge judiciaire comme c'est le cas dans les procès engagés sur le fondement du délit de contrefaçon.
En Italie, les opérateurs Internet[21]et téléphoniques sont tenus de conserver les données de connexion de leurs abonnés pendant soixante mois, soit cinq ans. Jusqu'en 2008, la loi stipulait que ces données de connexion devaient être stockées pendant trente mois. La norme présente change la donne. A partir de la troisième année, les données de connexion sont stockées sur des serveurs différents ; elles sont séparées des informations les plus récentes ; leur consultation est limitée ; seuls les services de police ou organismes d'Etat enquêtant sur le kidnapping, le crime organisé, le terrorisme, les délits informatiques peuvent y accéder
En Belgique, en 2001, avant les attentats du 11 septembre, la conservation des données de connexion a été fixée à un an.
En Espagne, la ley de Servicios de la Societad de la Informacion y de Comercio electronico[22] a été adoptée par le Parlement espagnol le 27 juin 2002 et est entrée en vigueur le 8 septembre 2002. La durée de conservation des données de connexion a été fixée à un an.
Au sein de l'Union européenne, la durée de conservation des données de connexion est très variable : trois ans pour la Lettonie[23], un an pour la Lituanie[24], un an pour la Pologne.

[20] Dans son chapitre deux
[21] Cf : décret du 28 janvier 2008
[22] Connue sous l'acronyme LSSICA
[23] Article 19 de la loi sur les communications électroniques du premier mai 2004
[24] Article 64 de la loi sur les communications électroniques du premier mai 2004

D'une façon générale, la conservation des données techniques pendant une certaine durée est entrée dans le corpus législatif des différents pays de l'Union européenne et la durée de conservation donne encore lieu à des débats.
Aux USA, les données de connexion sont en général conservées. Les moteurs de recherche enregistrent l'ensemble des données saisies par les utilisateurs et qui peuvent être rendues publiques sur injonction de justice. Les moteurs de recherche de Google, Yahoo, Microsoft conservent et archivent pour une durée non déterminée les mots saisis dans le champ « recherche » de ces moteurs. Seul AOL a décidé d'effacer ces données au bout de trente jours. Sont également enregistrés les liens de la page de résultats qui sont sélectionnés et visités par les utilisateurs. Par ailleurs, les données de connexion que sont l'adresse IP ciblée selon les centres d'intérêt des internautes, les applications pratiques afférentes à ces données sont prises en compte. Il est possible, sur simple injonction de la justice auprès du fournisseur d'accès, d'obtenir l'identité d'une personne à partir de son adresse IP et des horaires de connexion. En 2008, aucune loi n'a été débattue. Le Department of Justice peut accéder à ces informations sur injonction et est susceptible de lister les personnes qui ont saisi certains mots-clés à des fins de répression. De plus, les personnes physiques peuvent obtenir ces informations en sollicitant auprès du juge une injonction relative au moteur de recherche, dans le cadre d'affaires civiles, en dehors de toute incrimination pénale. La justice va dans le même sens, pour des affaires en relation avec le droit de la propriété intellectuelle. Le 29 mai 2006, TorrentSpy, site connu des amateurs de téléchargement a été condamné par un juge californien de Los Angeles à enregistrer les données de connexion relatives aux internautes qui le visitent, pour faciliter le travail de la MPAA[25]dans sa lutte contre le piratage des œuvres cinématographiques. La MPAA menait une bataille juridique depuis février 2006 contre des sites spécialisés dans l'hébergement et le référencement de liens torrent, tels TorrentSpy. Elle reprochait à ces sites de faciliter le piratage des œuvres cinématographiques. Les sites mis en cause ont fait valoir qu'ils usaient simplement de la liberté d'expression telle qu'elle est décrite dans le premier amendement de la Constitution américaine.

Qu'il s'agisse des interceptions traditionnelles (téléphone, mél) ou des données techniques, il est évident que les organismes de contrôle semblent amoindris depuis le début du vingt-et-unième siècle, bien que, dans certains cas, des entités de contrôle soient créées dans le cadre de lois plus ou moins liberticides. L'équilibre entre vie privée et sécurité penche, pour les organismes de contrôle comme pour les autres acteurs, en faveur de la sécurité.

Claudine Guerrier
Institut Telecom/TSMP (ex-INT)/ CEMANTIC

[25] Motion Picture Association of America