

LA CRYPTOLOGIE ENTRE SECURITE ET LIBERTE

Claudine Guerrier

La cryptologie, en 2004, tend à s'uniformiser. La liberté est le maître mot. Les différences entre les divers modèles, flagrantes dans les années 1990, libéralisme dans l'utilisation, l'importation, l'exportation (exemple : la Suède), libéralisme dans l'utilisation, mais pas dans l'exportation (exemple américain), refus de tout libéralisme (régimes autoritaires) tendent à s'estomper. Ceci s'explique par l'avènement du commerce électronique et le rapport de forces inversé entre industriels et armée. Les industriels l'ont emporté sur le lobby militaire parce que l'économie numérique avait besoin de sécurité dans ses transactions. Ainsi l'enjeu sécuritaire, omniprésent au début du vingt-et-unième siècle est-il le fil conducteur qui mène à la liberté économique.

La cryptologie, selon la Commission européenne, est « l'ensemble constitué par la conception des méthodes de chiffrement (cryptographie) et la recherche pour les casser (cryptanalyse) ».

En France, 2004 constitue une année charnière pour la cryptologie. Cette dernière a en effet, notamment sous sa forme cryptographique, été longtemps considérée comme une arme de guerre de deuxième catégorie. En conséquence, elle ne pouvait être utilisée, importée, exportée par aucune personne morale ou physique, sauf dérogation accordée par le chef de l'administration, le Premier ministre. La libéralisation a été très progressive et correspond aux deux étapes du processus européen de l'essor de la concurrence dans le secteur des télécommunications.

La première étape est celle de la première vague de libéralisation : terminaux, services à valeur ajoutée et est transcrite dans l'article 28 de la loi du 29 décembre 1990. Le texte fonde sa légitimité sur deux impératifs supérieurs : les intérêts de la défense nationale, la sécurité intérieure ou extérieure de l'Etat. Moyens et prestations de cryptologie ne sont plus prohibés ; ils sont soumis à un régime d'autorisation ou de déclaration préalable. La cryptologie en 1990 reste donc un modèle sécuritaire, mais respecte les droits des individus dans une démocratie.

La deuxième étape est celle de la deuxième vague de libéralisation : téléphonie fixe, infrastructures et est transcrite dans l'article 17 de la loi du 26 juillet 1996. Le système sécuritaire demeure, mais ses contours sont allégés, circonscrits. Il existe davantage de déclarations préalables et moins d'autorisations.

Par ailleurs, la France adhère à l'Arrangement de Wassenaar, qui a mis en place un contrôle des exportations des technologies à double usage¹. Il s'agit moins de multiplier les contrôles que de concentrer les investigations sur les prestations les plus sensibles. L'exportation se libéralise progressivement dans la plupart des Etats. Les USA, qui prônaient la liberté d'utilisation de la cryptologie au nom de la liberté d'expression garantie par le premier amendement de la Constitution, acceptent de libéraliser l'exportation des moyens et des prestations, des logiciels de cryptologie. Dans la mesure où la première puissance mondiale permet la sortie de ses produits cryptographiques, la France ne peut rester à l'écart du phénomène.

La libéralisation est d'abord introduite en France dans le domaine de l'utilisation sous le gouvernement Jospin. Elle n'est pas totale. Des carcans subsistent dans les secteurs de l'exportation, de la fourniture, de l'importation. La loi sur la confiance dans l'économie numérique (LCEN) du 21 juin 2004 essentiellement consacrée à l'Internet comprend un volet « télécommunications » et un volet « cryptologie ». L'objectif principal est celui de la liberté mais la sécurité demeure omniprésente : pour assurer de bonnes transactions, la liberté est nécessaire, mais des limites demeurent. La liberté n'est ni absolue, ni totale.

Si l'utilisation des moyens et des prestations de cryptologie est libéralisée, l'importation, le transfert, l'exportation demeurent soumis à des règles, des sanctions administratives et pénales sont prévues par la LCEN.

La liberté d'utilisation de la cryptologie n'est plus encadrée

Déjà, sous le gouvernement Jospin, la liberté d'utilisation avait progressé. Le critère de la longueur des clefs était retenu.

La liberté d'utilisation était totale, tant pour les personnes physiques que pour les personnes morales jusqu'à 40 bits, une longueur de clefs fort modeste. Cela signifiait que les personnes avaient accès à la liberté d'expression, pouvaient communiquer par code secret, si elles le souhaitaient. Rappelons que tous les codes secrets sont associés à une clef au moins pour le chiffrement et le déchiffrement. Pour que quelqu'un décode un message, il doit connaître la clef ; si elle est transmise par le réseau, elle peut être interceptée, elle est vulnérable. Conscients de cette faiblesse, deux chercheurs américains, Whitfield Diffie et Martin Hellman, ont inventé un système de code à deux clefs : l'une, publique, qui sert à chiffrer, l'autre privée, qui sert à déchiffrer. La clef publique peut transiter par les réseaux. La clef privée ne voyage pas.

¹ Civil et militaire

Entre 40 bits et 128 bits, la liberté d'utilisation était totale pour les personnes physiques. Les personnes morales, fournisseur, importateur, producteur devaient procéder à une déclaration préalable auprès de la DCSSI, la direction centrale de la sécurité des systèmes d'information, rattachée au Premier ministre.

Pendant cette période, les contraintes juridiques ne sont pas importantes. Malgré tout, les industriels, personnes morales, souhaitent ne pas avoir à formuler de déclaration préalable.

A partir de 2004, la liberté d'utilisation devient totale. Le concept de longueur de clefs est abandonné. Dans ce domaine, deux écoles s'opposent.

Certains insistent sur la sécurité induite par la longueur de clefs. Dans ce type de raisonnement, une longueur de clefs de 40 bits est insignifiante. Le code est facile à déchiffrer. A l'opposé, une clef de plusieurs milliers de bits serait quasiment inviolable, seuls des cryptanalystes particulièrement déterminés et expérimentés seraient en mesure de lever le secret du message. La vulgarisation médiatique a longtemps insisté sur cet aspect des choses.

Beaucoup de scientifiques et un certain nombre de journalistes ne croient pas que la longueur de clefs soit une panacée, une protection efficace. Les algorithmes cryptologiques peuvent être cassés relativement facilement. Les cryptanalystes contournent les algorithmes.

C'est la raison pour laquelle le critère longueur de clefs est abandonné non seulement pour l'utilisation, mais aussi pour le transfert, la fourniture, l'importation, l'exportation. La longueur des clefs n'est plus prise en compte par le législateur français. Cette dernière innovation a été bien acceptée par la presse et par les spécialistes de la cryptologie.

La liberté d'utilisation cryptologique satisfait à la fois les défenseurs des droits de l'homme et les tenants du libéralisme. La France, en adoptant la liberté d'utilisation de la cryptologie, s'aligne, avec beaucoup de retard, il est vrai sur les Etats qui concevaient que ladite liberté d'utilisation était une composante de la démocratie : les pays scandinaves (la Suède, le Danemark, la Norvège) et les pays qui, après avoir longtemps connu la dictature, s'étaient convertis à la démocratie et se montraient sourcilieux en matière de droits de l'homme (l'Espagne après Franco ; le Portugal après Salazar et la révolution des œillets). Désormais, la France ne se joint plus aux nations qui considèrent, pour des raisons de sécurité intérieure et extérieure, que l'utilisation de la cryptologie est réservée au ministère de l'intérieur et à l'armée comme la Chine, l'Iran, la Corée du Nord...

La liberté d'utilisation cryptologique est aussi une liberté économique, telle qu'elle a été définie par l'OCDE, l'OMC, le traité de Rome. Au sein de l'Union

européenne, le traité fondateur défend la liberté de circulation des produits, des marchandises, des services. Pour sécuriser leurs produits et leurs transactions, les commerçants ont besoin de logiciels de plus en plus performants, qu'ils soient en mesure d'utiliser immédiatement.

Cette liberté d'utilisation est l'aboutissement d'un long chemin qui a débouché sur le régime actuel.

La fourniture, le transfert, l'importation, l'exportation restent soumis à des règles

Le principe de liberté est adopté quand la cryptologie sert uniquement à des fonctions d'authentification et de contrôle d'intégrité. Dans les autres cas, il est fait recours à un régime d'autorisation et de déclaration.

La liberté s'applique à la fourniture, au transfert depuis ou vers un Etat membre de l'Union européenne, à l'importation ou à l'exportation pour les moyens de cryptologie qui assurent exclusivement des fonctions d'authentification ou de contrôle d'intégrité.

Les directives européennes de décembre 1999 sur la signature électronique et de juin 2000 sur le commerce électronique fixent les règles qui sont transposées dans chaque Etat. En France, il convient de citer la loi du 13 mars 2000 et le décret du 30 mars 2001. Ces règles s'appliquent aux contrats et à la signature électronique.

Les contrats électroniques ont la même valeur juridique que les contrats support papier. Les documents électroniques ont la même valeur probatoire que les documents support papier. Les documents électroniques sont des documents écrits. Si deux preuves sont contradictoires et sont pour l'une, un document électronique, pour l'autre, un document support papier, c'est au juge de déterminer souverainement quel est le titre le plus vraisemblable.

La signature électronique a la même valeur que la signature manuscrite. Elle matérialise le consentement des contractants.

Dans les deux cas, il convient de déterminer qui est à l'origine du document et de la signature. Les prestataires de services de certification (PSC) jouent un rôle essentiel en la matière. La cryptologie est utilisée et c'est pourquoi la liberté prévaut quand il s'agit d'authentification et de contrôle d'intégrité. Une fois de plus, il semble évident que le commerce électronique se doit de reposer sur la liberté.

La liberté est limitée lorsque la fourniture, le transfert, l'importation, l'exportation ne correspondent pas à une fonction d'authentification et de contrôle

d'intégrité et les régimes d'autorisation et de déclaration auprès du Premier ministre subsistent.

La fourniture, le transfert depuis un Etat membre de l'Union européenne (le terme « transfert » désigne les flux au sein de l'Union européenne ; l'exportation s'applique aux Etats étrangers), l'importation de moyens de cryptologie n'assurant pas de fonction d'authentification ou de contrôle d'intégrité, la fourniture de prestations de cryptologie sont soumis à un régime déclaratif auprès du Premier ministre.

Le transfert vers un Etat membre de l'Union européenne, les exportations de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation auprès du Premier ministre.

Néanmoins, des exceptions au régime d'autorisation et au régime déclaratif sont prévues :

- Quand, au regard des intérêts supérieurs de la défense nationale, de la sécurité de l'Etat, les moyens de cryptologie ne présentent aucune difficulté particulière, les autorisations peuvent laisser place à un régime déclaratif ou donner lieu à une dispense de formalités préalables.
- Lorsque les prestations de cryptologie présentent des caractéristiques techniques en harmonie avec les intérêts de la défense nationale, la sécurité intérieure ou extérieure de l'Etat, la fourniture de prestations peut être dispensée de toute formalité préalable.
- Ces exceptions sont définies par des décrets en Conseil d'Etat, qui vont jouer un rôle déterminant dans l'actuel statut de la cryptologie. Si les exceptions sont nombreuses, le régime de la cryptologie française pourra être considéré comme néo-libéral. Si les exceptions sont circonscrites, le régime de la cryptologie française sera mixte, libéral quant à l'utilisation, plus autoritaire quant à la fourniture, le transfert, l'importation, l'exportation.

L'importation et les logiciels libres

Les discussions parlementaires donnent lieu à de vives discussions sur les logiciels libres. Le sujet présente un intérêt à la fois économique et juridique.

Concernant les codes-sources des logiciels utilisés : le groupe socialiste, avec, notamment, comme porte-parole Jean-Yves Le Déaut dépose un amendement complétant l'importation par les mots suivants « ainsi que le code source des logiciels utilisés ». Il s'agit de garantir dans tous les cas que la puissance publique soit en mesure de contrôler les possibilités effectives des moyens cryptologiques en cause. Pour les parlementaires socialistes, cela permet de contrôler les caractéristiques techniques des produits utilisés pour la cryptologie. La ministre déléguée à l'Industrie, lors de la séance du 26 février 2003, renvoie aux textes d'application : le gouvernement n'aurait pas le recul indispensable. Le député socialiste Alain Gouriou insiste : il convient de faire

preuve de vigilance avec les codes-sources. Certains fournisseurs de logiciels de cryptologie n'hésiteront pas à détecter les failles de la législation. Cet argument a été repris par une dizaine de parlements dans le monde. L'amendement est finalement adopté en première lecture.

Concernant les logiciels libres et la cryptologie : les tenants des logiciels libres, représentés par des parlementaires socialistes, souhaitent dispenser de toute formalité préalable les logiciels de cryptologie diffusés publiquement à titre gratuit avec leur code source. Ainsi, un régime spécifique de liberté serait consenti aux logiciels libres de cryptologie. Pour les défenseurs de cet amendement, la recherche et l'innovation en cryptologie, tant pour les algorithmes liés à la recherche fondamentale que pour les applications impliquent une communication sans entraves entre chercheurs et toutes autres personnes concernées.

Le caractère public, ouvert, des échanges implique que les personnes publiques soient bien informées (ce qui est souhaitable) et puissent réagir si cela semble opportun. Les parlementaires ne représentent pas des intérêts, un lobbie privés. Ils sont les courroies de transmission de la recherche publique, notamment de l'INRIA, l'Institut national de recherche en informatique et en automatique, qui n'obéit pas à une logique de profit. Les chercheurs publics souhaitent continuer à échanger des algorithmes dans la transparence, à condition que les codes-sources soient connus et que le Gouvernement puisse procéder à des vérifications.

La loi, malgré les exceptions, limite l'importation et l'exportation de moyens de chiffrement. En conséquence, un noyau Linux ou un logiciel libre de chiffrement est passible de sanctions administratives, dans la mesure où ils peuvent être considérés comme des importations. Le rapporteur fait remarquer que la loi vise essentiellement des moyens de cryptologie, c'est-à-dire du matériel et des logiciels sous forme compilée. Or, les codes-sources, eux, constituent des textes et sont exclus du champ d'application de la loi. L'amendement est rejeté en première lecture. Il est de nouveau débattu en deuxième lecture. Alain Gouriou fait valoir que contrairement aux assertions gouvernementales, la publication d'un noyau Linux ou d'un logiciel libre est passible de sanctions administratives.

Par ailleurs, la question se pose de la compatibilité entre la loi française et l'Arrangement de Wassenaar. Ce dernier garantit la libre circulation d'œuvres et de documents issus de la recherche scientifique, des codes sources de chiffrement. Enfin, la loi peut décourager certains chercheurs spécialisés dans les logiciels libres et concourir à une émigration qui a déjà commencé. Une fois de plus, l'amendement est repoussé. Le gouvernement est favorable à l'interopérabilité. La normalisation internationale est grandement concernée. Les codes sources ne sont pas des moyens de cryptologie, ce sont des textes, dont il n'est pas question d'empêcher la diffusion. Le gouvernement s'engage à prendre en compte les diverses considérations soulevées et discutées à

l'occasion de l'élaboration des textes d'application, des décrets en Conseil d'Etat. Le logiciel OpenSSL a déjà bénéficié d'un régime déclaratif favorable pour son exportation et sa fourniture.

Responsabilité et garanties financières

(des personnes fournissant des prestations de cryptologie à des fins de confidentialité et des prestataires de services de certification).

Sauf exceptions (les personnes n'ont commis aucune faute intentionnelle ou négligence), les personnes qui fournissent des prestations de cryptologie à des fins de confidentialité sont responsables, au titre de ces prestations, des préjudices causés aux personnes qui leur confient la gestion de leurs conventions secrètes. Le projet de loi employait le terme « présumée responsable ». Un amendement rédactionnel supprime le mot litigieux, rend le texte plus clair et plus précis.

Les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées aux certificats présentés comme qualifiés lorsque les informations contenues dans le certificat, à la date de la délivrance, sont inexactes, lorsque les données sont incomplètes, quand la délivrance du certificat n'a pas donné lieu à la vérification, que le signataire détient la convention privée qui correspond à la convention publique du certificat. Dans les directives de décembre 1999 sur la signature électronique et de juin 2000 sur le commerce électronique, la responsabilité des prestataires de services de certification est mentionnée clairement. Elle n'est pas reprise, en dépit des critiques de la doctrine, par le décret du 30 mars 2001. Il faut donc attendre 2004 et la LCEN pour assister à la transposition des textes européens.

Les garanties financières pour les prestataires de services de certification sont précisées : ces derniers, ceci dans un souci de protection du client, doivent assumer les conséquences de la responsabilité et être en mesure d'honorer la réparation du préjudice. La garantie financière est « suffisante », elle est spécialement affectée au paiement des sommes dues ; la LCEN envisage aussi l'établissement d'une assurance qui garantit les conséquences pécuniaires de la responsabilité civile et professionnelle.

A l'occasion des débats, tant en première lecture qu'en deuxième lecture, les députés socialistes souhaitent que soit envisagée l'absence de garantie financière ou d'assurance. En première lecture, un amendement, n° 147, est présenté. Pour que les clients ne soient pas pris au dépourvu, les certificats délivrés par les prestataires de service de certification doivent comporter une mention de l'absence de garantie financière ou d'assurance. Selon Alain Gouriou, qui représente le groupe socialiste, cet amendement apporte davantage de clarté, donc de bonne foi, entre le client et le prestataire de service de certification. Le rapporteur considère que cet amendement a

une vertu dissuasive. Le fait même de mentionner, pour la compréhension du client, qu'il n'existe pas de garantie financière ou d'assurance sera un puissant facteur d'incitation à l'égard des prestataires de service de certification qui, dans leur quasi-unanimité, souscriront une garantie financière ou une assurance. Le Gouvernement manifeste ses réserves : pourquoi faire mention d'une obligation non respectée ? Toutefois, il ne s'oppose pas à cet amendement qui est adopté en première lecture par l'Assemblée nationale.

En deuxième lecture, un nouvel amendement, n° 67, est présenté sur le même thème par le groupe socialiste. Le rapporteur considère qu'il n'est pas très logique de faire mention d'un manquement à une obligation. Toutefois, cet amendement permet une meilleure information du client, dans ses relations avec le prestataire de services de certification. La ministre déléguée à l'Industrie s'appuie sur le défaut de logique. Finalement, le rapporteur se rallie à la ministre. L'amendement n'est pas adopté en deuxième lecture. Entre une belle et bonne fluidité rédactionnelle et un souci d'information / compréhension pour le client face au professionnel, le prestataire de services de certification, c'est la fluidité rédactionnelle qui l'emporte auprès du législateur.

La LCEN prévoit des sanctions administratives et pénales

Ces sanctions ne sont pas seulement symboliques. Elles ont un caractère dissuasif. Il reste à déterminer si ces sanctions seront appliquées. Dans les lois concernant la libéralisation des télécommunications et dans la loi du 6 janvier 1978, récemment modifiée, les sanctions ont été rarement appliquées. Les sanctions prévues dans les étapes antérieures, loi du 29 décembre 1990 et loi du 26 juillet 1996, ont été rarement mises en vigueur. Il ne semble pas que le contexte de 2004 soit plus favorable à des condamnations que le contexte de 1990 et celui de 1996.

Les sanctions administratives

Les sanctions sont parfois administratives : ces sanctions administratives concernent essentiellement les fournisseurs de moyens de cryptologie. Quand un fournisseur ne respecte pas les dispositions légales, le chef de l'administration, le Premier ministre, qui dispose d'une compétence particulière dans le domaine de la cryptologie, peut, après avoir donné à l'intéressé le moyen d'exprimer ses observations, interdire la mise en circulation du moyen de cryptologie concerné.

Le fournisseur doit en outre procéder au retrait, auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été prohibée, et

des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis par l'intermédiaire de diffuseurs.

En première lecture, le rapporteur propose un amendement. La prohibition de la mise en circulation paraît trop vaste, donc difficilement applicable. Le retrait est difficile pour des logiciels qui peuvent faire l'objet d'une contrefaçon. L'identité des utilisateurs doit être déterminée ; elle est délicate à établir lorsque la diffusion a été réalisée à titre gratuit. L'obligation de retrait s'applique donc auprès des diffuseurs commerciaux des matériels et logiciels ; les matériels concernés, par exemple les téléphones chiffrés, sont obtenus à titre onéreux. L'amendement, qui a le mérite de la précision, est adopté.

Le groupe socialiste présente un amendement, n° 148, qui ouvre des perspectives. Le moyen de cryptologie pourrait être remis en circulation dès que les obligations, qui n'ont pas été respectées, auront été satisfaites. Cet amendement relaie les inquiétudes de certains fournisseurs. En effet, il ne convient pas que les manquements d'un fournisseur puissent nuire à d'autres fournisseurs, dans la mesure où certains moyens de cryptologie sont diffusés à l'identique par plusieurs fournisseurs différents. Le rapporteur fait remarquer que la précision va de soi et qu'elle n'apporte pas d'amélioration rédactionnelle. L'amendement est donc rejeté.

Les sanctions pénales

Les sanctions sont aussi, dans d'autres cas, pénales. Le refus de souscrire à des modalités de déclaration ou d'autorisation est puni d'un an d'emprisonnement (déclaration), de deux ans d'emprisonnement (autorisation) et de peines d'amende.

Des peines complémentaires sont prévues : interdiction, pour une durée de cinq ans au maximum, d'émettre des chèques et d'utiliser des cartes de paiement ; la chose qui a permis de commettre l'infraction est confisquée ; il est interdit, pendant une durée de cinq ans au maximum, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise ; l'établissement où l'infraction a eu lieu est fermé pour une durée de cinq ans maximum. Cet ensemble de mesures est très sévère. Il reste à déterminer si ces sanctions pénales seront appliquées.

Les personnes qui sont habilitées à dresser procès-verbal sont les officiers et agents de police judiciaire agissant conformément au code de procédure pénale, les agents des douanes agissant conformément au code des douanes, et les agents dépendant du Premier ministre, assermentés dans des conditions fixées par décret en Conseil d'Etat. Sur ce point, les débats parlementaires sont assez vifs. Le groupe socialiste dépose, en première lecture devant l'Assemblée nationale un amendement visant à supprimer ce corps spécifique d'hommes et de femmes spécialisés dans la cryptologie et dépendant du Premier ministre : ces agents sont en dehors du droit commun. Néanmoins, le rapporteur est favorable à cette structure. En effet, la constatation des

infractions en cryptologie est spécifique. La complexité du domaine justifie la création d'agents spécialisés. L'amendement n'est pas adopté mais il est de nouveau présenté en deuxième lecture devant l'Assemblée nationale. Alain Gouriou, pour le Parti socialiste insiste sur le caractère superflu de ces agents ; il craint aussi une dérive : cette disposition pourrait servir d'instrument afin d'organiser des perquisitions pour lesquelles la référence à la cryptologie ne serait qu'un prétexte. Le rapporteur souligne qu'il est opportun d'envisager un corps d'agents spécialisés dépendant exclusivement du Premier ministre. Le SGDN et le service central de la Sécurité des systèmes d'information sont rattachés au Premier ministre. Ce dernier, de par sa fonction, mais aussi de par ses services très compétents dans tout ce qui relève de la société de l'information, dispose d'une compétence affûtée en cryptologie. Or, la cryptologie est hautement technique et implique, dans la lutte contre les infractions, des connaissances pointues en cryptographie et en cryptoanalyse. L'amendement est donc repoussé. Le danger dans le secteur des libertés individuelles est relativement limité surtout si l'on se réfère à la loi sur la sécurité quotidienne et à la loi sur la sécurité intérieure.

Lorsqu'une infraction est commise à l'aide d'un moyen de cryptologie, la peine est plus lourde. Par exemple, le maximum de la peine privative de liberté est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ; il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle.

Le Parti socialiste dépose un amendement (première et deuxième lecture devant l'Assemblée nationale) pour supprimer cet article. En effet, dans la mesure où l'utilisation de la cryptologie est libre, il semble illogique d'aggraver les peines quand elles sont commises avec l'aide de la cryptologie. Le rapporteur rappelle que le texte est basé d'une part sur la liberté totale d'utilisation de la cryptologie, d'autre part, sur une aggravation des peines prévues quand il y a manquement à une obligation légale en cryptologie. De plus, ces infractions ralentissent le travail de la justice. Il convient de le prendre en compte.

Les dispositions très sévères que nous avons évoquées dans le paragraphe précédent ne sont pas applicables à l'auteur ou au complice de l'infraction, qui, à la demande des autorités judiciaires ou administratives, leur a remis en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement. Ce paragraphe concerne le statut des «repentis» en cryptologie qui acceptent de collaborer avec la justice après avoir commis une infraction. Ce statut du repentis est mis en cause par le groupe socialiste. En effet, la France a signé le 4 novembre 1980 le pacte international relatif aux droits civils et politiques. Dans son article 14, le pacte stipule que toute personne accusée d'une infraction pénale a droit à certaines garanties, parmi lesquelles figure le droit à ne pas être forcée de témoigner contre elle-même ou de s'avouer coupable. Le statut des repentis existe en France, dans quatre cas : les trafics de fausse

monnaie et de stupéfiants, les actes de terrorisme, les évasions, les crimes et les délits relevant de la criminalité organisée. Il s'agit de prévoir un cinquième cas : les collaborateurs de la justice viennent au secours de la lutte contre la cybercriminalité. Les points de vue sont inconciliables : pour les uns, les repentis, qui collaborent avec la justice ne doivent pas supporter une aggravation de la peine qui se justifie par le ralentissement des procédures. Pour les autres, une nouvelle exception, peu justifiée, vient s'ajouter aux cas des repentis, qui ne sont pas en concordance avec l'esprit du code de procédure pénale.

Le nouveau droit de la cryptologie français est donc assez complexe. Il est loin d'être complètement libéral. Il tempère le principe de liberté d'utilisation avec les régimes de déclaration et d'autorisation. Il faut attendre la sortie des décrets en Conseil d'Etat pour savoir si ce nouveau droit de la cryptologie penche plutôt du côté de la liberté, ou plutôt du côté de la sécurité.