
SECURITE, CRYPTOLOGIE ET LIBERTES

Par [Eric A. Caprioli](mailto:eric.a.caprioli@caprioli-avocats.com)

[e.caprioli@caprioli-avocats.com](mailto:eric.a.caprioli@caprioli-avocats.com)

PLAN

[Introduction](#)

[I/ Déchiffrement et procédure pénale](#)

[II/ Déchiffrement et interceptions de sécurité](#)

[III/ Obligations de remettre et de mettre en œuvre les conventions secrètes](#)

[Notes](#)

Introduction

Dès lors que l'on entend préserver des informations confidentielles établies sous forme de fichiers ou de données électroniques, et qu'elles sont transmises par voie électronique au travers de réseaux numériques ouverts, l'utilisation de moyens de cryptologie s'impose. Ces secrets peuvent relever du domaine bancaire, de la défense ou de l'Etat, de professionnels (avocats, médecins), des affaires ou de la vie privée. Les technologies à base de cryptologie sont également employées pour le stockage et la conservation des informations secrètes en local (disques durs, disques optiques numériques, ...), ainsi que pour la protection des droits des auteurs et des cessionnaires sur les œuvres numériques destinées à circuler sur les réseaux ([\[1\]](#)).

Dans le commerce électronique ([\[2\]](#)) la confiance repose pour l'essentiel sur la sécurité offerte par la cryptologie et sur l'intermédiation assurée par les tiers de confiance.

Techniquement, cette « science du secret » se décompose en trois fonctions principales : confidentialité, « authentification » et intégrité. En termes juridiques, la fonction de confidentialité est associée au chiffrement du contenu du message alors que les fonctions d'authentification et d'intégrité relèvent de la signature électronique. Cette distinction établie par la loi a des conséquences pratiques importantes, spécialement en ce qui concerne les aspects réglementaires relatifs aux fonctionnalités des moyens de cryptologie utilisés.

Quelques semaines après les attentats du 11 septembre 2001, le gouvernement a proposé au Parlement le projet de loi sur la sécurité au quotidien (L.S.Q.), dont certaines parties, applicables à la société de l'information, ont été extraites du projet de loi sur la société de l'information (Juin 2001). Les sujets abordés témoignent des priorités politiques de l'État :

- * L'instauration de procédures de déchiffrement des fichiers chiffrés dans le cadre de leur découverte au cours de l'enquête pénale ainsi que dans le cadre des procédures d'interception de sécurité en vertu de la loi du 10 juillet 1991 (articles 30 et 31 de la LSQ) ;
- * et la conservation des données de connexion des internautes par les opérateurs de télécommunications pendant une durée de un an avec pour finalité de mettre à la disposition des autorités judiciaires les informations nécessaires à l'enquête (article 29 de la LSQ, modifiant l'article L. 32-3 du Code des Postes et Télécommunications).

Il convient de préciser que la Loi de finances rectificative pour 2001 en date du 28 décembre 2001 a élargi l'accès aux données de connexion auprès des fournisseurs d'accès et des opérateurs de télécommunications, aux agents des douanes, du fisc et aux enquêteurs de la Commission des Opérations de Bourse (COB) contrairement à la LSQ qui réservait cette possibilité aux seuls juges ([\[3\]](#)).

Le projet de loi fut adopté par le Sénat et l'Assemblée les 17 et 31 octobre 2001. La publication de la loi a quelque peu tardé puisqu'elle est datée du 15 novembre ([\[4\]](#)).

Les dispositions sur la cryptologie figurent dans un Chapitre V au titre évocateur : « Dispositions renforçant la lutte contre le terrorisme ». L'article 22 trace la perspective dans laquelle s'inscrivent les dispositions légales : « Afin de disposer des moyens impérieusement nécessaires à la lutte contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication, les dispositions du présent chapitre sont adoptées pour une durée allant jusqu'au 31 décembre 2003. Le Parlement sera saisi par le Gouvernemen, avant cette date, d'un rapport d'évaluation sur l'application de l'ensemble de ces mesures. ».

On observera que les mesures sont prises dans un contexte particulier, à titre provisoire et qu'elles feront l'objet d'une évaluation de leur application. Gageons que c'est leur efficacité qui sera prise en compte avant qu'elles ne soient reconduites ou abrogées. Mais toute la question reposera sur les moyens mis en oeuvre. Cependant, le Ministre de l'intérieur de l'époque a pris un engagement : celui de répondre à tous

moments aux questions du Parlement concernant l'application de ces mesures, « *et à cette fin, le Gouvernement est prêt à présenter un rapport d'évaluation à la fin de l'année 2002* » (51). Le sujet est sensible, certaines associations et certains syndicats (l'association Iris, le Syndicat de la Magistrature et la Ligue des droits de l'homme notamment) ont parlé à propos du projet, de loi liberticide, de loi d'exception « *gravement attentatoires aux libertés fondamentales* », voire de loi « *de surenchère sécuritaire sur Internet* ».

En ce qui concerne la remise des conventions secrètes auprès d'une tierce partie de confiance en qualité de séquestre agréé, on peut s'interroger sur l'avenir de cette activité dans la mesure où, désormais, la loi prévoit la possibilité de faire déchiffrer les outils cryptographiques utilisés dans le cadre de la procédure pénale (I) et des interceptions de sécurité (II). En outre, la loi impose la remise et/ou la mise en œuvre des conventions secrètes (ex : les clés de déchiffrement) aux autorités judiciaires (III). Ces dispositions légales interpellent l'avocat, tant en terme technique qu'en terme de libertés fondamentales.

I / Déchiffrement et procédure pénale

L'article 30 de la loi introduit cinq articles (articles 230-1 à 230-5 du Code de procédure pénale) aux termes desquels, les magistrats saisis d'une affaire (le parquet, le juge d'instruction ou la juridiction de jugement) ont le pouvoir d'ordonner le déchiffrement des données (messages et fichiers). Le texte reprend celui qui figurait à l'article 47 de la Loi sur la société de l'information (L.S.I.). L'objectif est de donner aux magistrats chargés de l'enquête ou de l'instruction ainsi qu'à la juridiction de jugement saisis les moyens d'accéder au clair du contenu des messages chiffrés.

Ainsi, les juges pourront recourir aux services d'expert en cryptologie (« *toute personne physique ou morale qualifiée* »), ainsi qu'aux « *moyens de l'Etat couvert par le secret de la défense nationale* ». Comme le relevait le Ministre de la Justice, « *Dans les cas les plus sophistiqués de cryptologie, le déchiffrement des messages en tre membres des réseaux terroristes suppose le recours à des experts de très haut niveau voire à des moyens de l'Etat couverts par le secret défense nationale. Il est donc nécessaire d'organiser le recours à ces moyens de manière à assurer leur fiabilité juridique dans le cadre d'une procédure pénale.* » (61).

Le recours aux services d'un prestataire, séquestre des conventions secrètes (la Tierce Partie de Confiance) est régi par la loi n°90-1170 du 29 décembre 1990 et les décrets d'application du 24 février 1998 et du 17 mars 1999. L'un des décrets de 1999 libéralisant l'utilisation des moyens de cryptologie pour des longueurs de clés symétriques inférieures ou égales à 128 bits, n'annule pas ces dispositions légales et réglementaires. De plus, non seulement le recours à un séquestre demeure toujours possible quelle que soit la longueur des clés utilisées, mais ledit recours peut également relever d'un contrat conclu entre le titulaire de la clé et un Prestataire de service de certification électronique (si ce service est proposé).

Rappelons que par « *conventions secrètes* », on entend : « *des clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement.* » Et que la « *gestion de conventions secrètes* », c'est « *la détention, la certification, la distribution ainsi que, éventuellement, la génération des clés dans des conditions définies au cahier des charges prévu par l'article 8.* » Enfin, la « *certification de conventions secrètes* », c'est « *l'opération qui consiste à calculer une signature numérique ou un code d'authentification assurant la faculté d'emploi des conventions secrètes.* » (71).

Concernant la procédure, dans le premier cas le magistrat désigne « *toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire* » (article 230-1 al. 1^{er} du C.P.P.).

Dans le second cas qui implique le recours aux moyens de l'Etat couverts par le secret de la défense, le texte prévoit une procédure renforcée, « *si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent* » (article 230-1 al. 2 du C.P.P.). Etant donné le caractère et l'importance des moyens mis en œuvre, il est envisagé le recours « *à un organisme soumis au secret de la défense nationale* ». De plus, la procédure se réalise sous forme écrite. Selon l'article 230-1, une telle opération comporte le double objectif d'obtenir la version en clair des informations et, lorsqu'un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement. Les données visées par le texte sont protégées d'une double manière. Au moment de la communication à l'organisme technique chargé des opérations, les données sont protégées au titre de la défense nationale et leur communication doit être faite dans les conditions prévues par la loi du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale. Ces données sont également protégées après avoir été soumises aux opérations techniques. Le texte exige ainsi que les résultats accompagnés des indications techniques permettant de les comprendre et de les exploiter soient retournés aux services de police judiciaire qui les avait transmis. Enfin, l'organisme technique doit adjoindre une attestation certifiant la sincérité des résultats transmis. On peut s'interroger sur les moyens dont disposent les prévenus pour vérifier le contenu de ces attestations dès lors qu'elles relèvent du secret défense et que certains expert en sécurité des systèmes d'information estiment qu'il est impossible d'accéder au clair selon les technologies utilisées.

Le nouveau texte impose également qu'un délai soit spécifié pour chaque type d'opération. Ce délai est fixé par la réquisition et peut faire l'objet d'une prorogation. Cependant, en pratique les opérations de déchiffrement peuvent, soit demander une période plus importante que celle spécifiée par la réquisition, soit même se révéler impossibles du point de vue technique. Dans tous les cas, l'organisme technique est soumis à une obligation de restituer les résultats obtenus. A cet égard, le texte ne contient aucune

disposition relative aux garanties sur les conditions et les résultats de l'opération de déchiffrement des messages.

La procédure nécessite l'intervention de plusieurs entités, en fonction de la nature des moyens à utiliser. Ainsi, dans la variante simple, le procureur de la République ou le juge désigne directement une personne pour effectuer les opérations techniques nécessaires. Dès lors que des moyens couverts par le secret de la défense nationale sont nécessaires, le système comporte un intermédiaire. Ainsi l'Office central de la lutte contre la criminalité liée aux technologies de l'information se charge de transmettre la demande de déchiffrement à un service de police judiciaire qui la transmet à un organisme technique. Le retour des informations emprunte la même voie.

Enfin, il convient de remarquer que ces mesures d'instruction ne sont pas susceptibles de recours comme l'article 230-4 du C.P.P. le rappelle. Ainsi, « *les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.* » ...

II/ Déchiffrement et interceptions de sécurité

Les autorités judiciaires pourront avoir accès aux conventions de chiffrement des données chiffrées par le présumé délinquant par l'entremise des prestataires de services de cryptologie. Le nouvel article 11-1 de la loi du 10 juillet 1991 impose cette obligation de remise aux agents autorisés dans les conditions prévues à l'article 4 de ladite loi, « *l'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de la personne que chacun d'eux aura spécialement déléguée. Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées.* »

Néanmoins, les procédures de déchiffrement s'inscrivent dans le cadre de l'article 3 de la loi du 10 juillet 1991, c'est-à-dire qu'elles concernent exclusivement « *des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la constitution ou du maintien de groupements dissous.*» ([18](#))

Le texte vise les prestataires de façon plus large que dans le projet de L.S.I. qui faisait porter les obligations sur ceux dont les prestations incluaient « *la gestion de convention secrète* ». Aujourd'hui, il apparaît que tous les prestataires sont concernés à partir du moment où ils fournissent des prestations de cryptologie. Ainsi, toute personne qui procède à l'utilisation de la cryptographie dans la diffusion d'un message quelconque pourrait être visée par cet article. En pratique, il existe des logiciels de cryptographie (ex. OpenPGP) qui permettent à l'expéditeur, et en conséquence au destinataire, de garder secrète la convention utilisée sans qu'un prestataire n'intervienne. De la sorte, aucun fournisseur de cryptologie ne possède jamais une copie de cette convention. Dans une perspective identique, un prestataire (PSCE) qui héberge les clés privées de ses clients pourrait être contraint de les remettre, étant précisé que techniquement, on ne peut pas brider la fonction de chiffrement des bi-clés de signature électronique. A notre avis, le champ d'application de cet article se révèle trop extensif et soulève des questions de libertés fondamentales assez importantes. Il faut cependant trouver un équilibre entre les besoins de protection de l'Etat et les droits et libertés individuels.

En cas de non remise ou de non mise en œuvre des conventions permettant de déchiffrer les données conformément à la demande, les personnes sont passibles de deux ans d'emprisonnement et de 30 000 € d'amende (article 11-1 al. 3). Le décret n°2002-997 du 16 juillet 2002 ([19](#)) vient de préciser les procédures de mise en œuvre de ces obligations ainsi que la compensation financière qui devra être assurée par l'Etat en application de l'article 11-1 al. 3. C'est l'intégralité des frais liés à l'obligation de mise en œuvre qui sera compensée, « *sur la base des frais réellement exposés par le fournisseur et dûment justifiés par celui-ci* » (article 6 du décret). Selon l'article 3 du décret, « *les conventions mentionnées (...) permettant le déchiffrement des données s'entendent des clés cryptographiques ainsi que de tout moyen logiciel ou de toute autre information permettant la mise au clair de ces données* ». Une telle définition est très large ; elle vise non seulement toutes les clés de déchiffrement (symétriques et asymétriques), mais aussi les services de messagerie chiffrée, voire les procédés de signature électronique et d'authentification.

III/ Obligations de remettre et de mettre en œuvre les conventions secrètes

Le nouvel article 434-15-2. du Code pénal établit une nouvelle incrimination, reprenant mot pour mot l'article 46 du projet de L.S.I. On observera en cet endroit qu'il est positionné au titre des entraves à la justice. Aux termes de cet article deux hypothèses doivent être distinguées :

1°) « Est puni de trois ans d'emprisonnement et de 45.000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale. »

Cela concerne toutes les personnes amenées à connaître une convention secrète, c'est à dire le titulaire, l'émetteur, le ou les destinataire(s) des messages chiffrés et les prestataires de services de

cryptographie ce qui à notre avis touche également ceux qui fournissent des clés de signature asymétriques ; puisque les certificats à clés publiques sont, en effet, susceptibles d'être utilisés à des fins de confidentialité pour le chiffrement avec la clé publique vers le titulaire de la clé privée.

Le texte vise à la fois le refus de remettre les conventions secrètes aux autorités et le refus de les mettre en œuvre. Dès lors, comment faire si l'on a perdu ou détruit involontairement la clé de déchiffrement et que l'on se trouve *de facto* dans une situation où la personne veut s'acquitter de ses obligations légales mais qu'elle ne le peut pas ?

Par ailleurs, il existe un principe en matière de liberté publique qui énonce que les individus accusés d'avoir commis une infraction, ne peuvent être obligés ni de témoigner contre eux-mêmes, ni d'avouer leur culpabilité ([10]). En conséquence, cet article pourrait être déclaré non conforme à la Convention européenne des droits de l'homme.

2°) « Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75.000 € d'amende. »

Dans cette seconde hypothèse, les sanctions sont plus lourdes. Toutefois, on est en droit de s'interroger quant à l'établissement de la preuve de la conséquence « *aurait permis d'éviter la commission, ..., ou d'en limiter les effets* ». En effet, il semble difficile, *a priori*, d'établir cette preuve sans que l'on ait accès au contenu du message chiffré. Bien entendu, le juge bénéficiera d'un faisceau d'indices tendant à établir la culpabilité de l'auteur présumé pour forger son intime conviction. Mais il n'en demeure pas moins, qu'il ne lui sera pas possible d'en avoir la certitude. Il conviendra de veiller au respect des droits de la défense afin d'éviter d'éventuelles mesures arbitraires.

Si l'on replace cet article du code pénal dans le contexte de la LSI, on peut estimer qu'il se justifiait pour contrebalancer la libéralisation (totale) de l'utilisation des moyens et prestations de cryptologie ([11]). Or, à ce jour, l'utilisation des moyens et des prestations de cryptologie reste limitée à des clés inférieures ou égales à 128 bits. Envisagé sous cet angle, cet article a pour but exclusif de donner des moyens supplémentaires de lutte en matière de terrorisme et de grande criminalité.

Ceci nous conduit à rappeler que les textes de droit pénal sont d'interprétation stricte et qu'à ce titre la remise et la mise en œuvre des conventions secrètes ne sont pas admissibles en dehors des actes qualifiés par le législateur de terrorisme alimenté notamment par le trafic de stupéfiant et les trafics d'armes. L'application de ces nouvelles règles dans les affaires pénales invitent les avocats à la vigilance dans le cadre de la sauvegarde des droits et libertés de leurs clients.

Notes :

[1] Eric A. Caprioli, *Dispositifs techniques et droit d'auteur dans la société de l'information*, in *Mélanges offerts à Jean-Pierre Sortais*, Bruxelles, Bruylant, 2002.

[2] Lamy droit des médias et de la communication, Eric A. Caprioli, Anne Cantéro et Xavier Le Cerf, *Commerce électronique*, mai 2002, Étude 468.

[3] Cela figure à l'article 62 de la LFR n° 2001-1276, adoptée le 28 décembre 2001, J.O. du 29 décembre 2001, p. 21133 s.

[4] J.O. du 16 novembre 2001, p. 18214 s.

[5] J.O.A.N., 1^{er} novembre 2001, p. 6992 s.

[6] J.O. Sénat, 18 octobre 2001, v. p. 4149.

[7] Décret n° 98-102 du 24 février 1998 (JO du 25 février 1998, p. 2915).

[8] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, J.O. du 13 juillet 1991

[9] J.O. du 18 juillet 2002, p. 12255.

[10] Article 14, 3° du Pacte international relatif aux droits civils et politiques de New York 16 décembre 1966, entré en vigueur le 18 septembre 1992, publié par le décret n° 81-76 du 29 janvier 1981.

[11] L'article 37-I du projet de L.S.I. disposait : « *L'utilisation des moyens de cryptologie est libre.* »
L'article 37-II allait dans un sens identique, mais plus large quant aux finalités d'utilisation des fonctions d'authentification et d'intégrité : « *La fourniture, le transfert depuis ou vers un États membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie dont la seule fonction cryptologique est une fonction d'authentification ou de contrôle d'intégrité, notamment à des fins de signature électronique, sont libres.* »